UNIVERSITY OF OULU

FACULTY OF TECHNOLOGY

CONNECTED VEHICLES – ORGANIZATIONAL CYBERSECURITY PROCESSES AND THEIR EVALUATION

Harri Juutilainen

INDUSTRIAL ENGINEERING AND MANAGEMENT

Master's thesis

May 2023

ABSTRACT

Connected vehicles – organizational cybersecurity processes and their evaluation

Harri Juutilainen

University of Oulu, Master's program of Industrial Engineering and Management

Master's thesis 2023, 77 pp. 1 appendix

Supervisors at the university: D.Sc.(Tech) Hannele Lampela, D.Sc.(Tech) Arto Reiman

Vehicles have become increasingly network connected cyber physical systems and they are vulnerable to cyberattacks. In the wake of multiple vehicle hacks, automotive industry and governments have recognized the critical need of cybersecurity to be integrated into vehicle development framework and get manufactures involved in managing whole vehicle lifecycle. The United Nations Economic Commission for Europe (UNECE) WP.29 (World Forum for Harmonization of Vehicle Regulations) committee published in 2021 two new regulations for road vehicles type approval: R155 for cybersecurity and R156 for software update. The latter of these influence also to agricultural vehicle manufacturers, which is the empirical context of this study. Also new cybersecurity engineering standard from International Standardization Organization (ISO) and Society of Automotive Engineers (SAE) organizations change organizations risk management framework. The vehicle manufacturers must think security from an entirely new standpoint: how to reduce vehicle cybersecurity risk to other road users. This thesis investigates automotive regulations and standards related to cybersecurity and cybersecurity management processes. The methodology of the empirical part is design science that is a suitable method for the development of new artifacts and solutions. This study developed an organization status evaluation tool in the form of a questionnaire. Stakeholders can use the tool to collect information about organizational capabilities for comprehensive vehicles cybersecurity management process. As a main result this thesis provides base information for cybersecurity principles and processes for cybersecurity management, and an overview of current automotive regulation and automotive cybersecurity related standards.

Keywords: Cyber physical systems, automotive, cybersecurity, standards

TIIVISTELMÄ

Verkotetut ajoneuvot – organisaation kyberturvallisuusprosessit ja niiden arviointi

Harri Juutilainen

Oulun yliopisto, Tuotantotalouden diplomi-insinöörin tutkinto-ohjelma

Diplomityö 2023, 77 s. + 1 liite

Työn ohjaajat yliopistolla: TkT. Hannele Lampela, TkT. Arto Reiman

Ajoneuvoista on tullut kyberhyökkäyksille alttiita tietoverkkoon yhdistettyjä kyberfyysisiä järjestelmiä. Ajoneuvojen hakkeroinnit herättivät hallitukset ja ajoneuvoteollisuuden huomaamaan, että kyberturvallisuus on integroitava osaksi ajoneuvojen kehitysympäristöä ja valmistajat on saatava mukaan hallitsemaan ajoneuvon koko elinkaarta. Yhdistyneiden Kansakuntien Euroopan talouskomission (UNECE) WP.29 (World Forum for Harmonization of Vehicle Regulations) -komitean jäsenet julkaisivat vuonna 2021 kaksi uutta tyyppihyväksyntäsäädöstä maantiekäyttöön tarkoitetuille ajoneuvoille. Nämä ovat kyberturvallisuuteen R155 ja ohjelmistopäivitykseen R156 liittyvät säädökset, joista jälkimmäinen vaikuttaa myös maatalousajoneuvojen valmistajiin. Myös uusi International Standardization Organization (ISO) ja Society of Automotive Engineers (SAE) organisaatioiden yhdessä tekemä kyberturvallisuuden suunnittelustandardi muuttaa organisaatioiden riskienhallintaa. Ajoneuvovalmistajien on pohdittava turvallisuutta aivan uudesta näkökulmasta; kuinka pienentää ajoneuvojen kyberturvallisuusriskiä muille tienkäyttäjille. Tämä opinnäytetyö tutkii kyberturvallisuuteen liittyviä autoalan säädöksiä ja standardeja sekä kyberturvallisuuden johtamisprosesseja. Työn empiirinen osa käsittelee maatalousajonevoihin erikoistunutta yritystä. Empiirisen osan metodologia on suunnittelutiede, joka soveltuu uusien artefaktien ja ratkaisujen kehittämiseen. Tutkimuksen empiirisessä osassa kehitettiin uusi arviointityökalu, jolla sidosryhmät voivat kerätä tietoja organisaation valmiuksista ajoneuvojen kyberturvallisuuden hallintaan. Tämä opinnäytetyö tarjoaa pohjatietoa kyberturvallisuuden periaatteista ja kyberturvallisuuden hallinnan prosesseista sekä yleiskatsauksen nykyiseen autoalan sääntelyyn ja kyberturvallisuuteen liittyviin ajoneuvostandardeihin.

Asiasanat: kyberfyysiset järjestelmät, ajoneuvot, kyberturvallisuus, standardit

FOREWORD

This master's thesis is done in co-operation with ACGO corporation department of electronic functional group (EFG) for the University of Oulu Faculty of Technology master's program of Industrial Engineering and Management. The work has been very interesting because ongoing digitalization transformation makes cybersecurity one of the key perspectives to new vehicle product development. New cybersecurity regulations have become effective in the automotive domain and manufacturers have to implement a new framework for their development processes. After some delay similar processes will come to other road vehicle manufacturers. New framework implementation to organizational processes is a challenging topic.

I want to express my thanks to AGCO Corp. and to my instructor M.Sc. Nicolas Meunier and also to professors at the University of Oulu. I also want to express my gratitude to the supervisors at the university Hannele Lampela and Arto Reiman who have given excellent guidance and support through the thesis process.

Jyväskylä, 7.5.2023

Harri Juutilainen
Author

TABLE OF CONTENTS

APPENDICES:

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
CAL	Cybersecurity Assurance Level
CAN/CAN FD	Controller Area Network/Controller area network Flexible Data-rate
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIA	Confidentiality, Integrity and Availability -attributes
C-ITS	Cooperative Intelligent Transport Systems
CSMS	Cyber Security Management System
CPS	Cyber Physical System
DAD	Disclosure, Alteration and Denial -attributes
DIN	Deutsches Institut für Normung e. V.
DMZ	Demilitarized Zone
ECU	Electronic Control Unit
E/E	Electrical and Electronic systems
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle
GNSS	Global Navigation Satellite System
GSR	Vehicle General Safety Regulation
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Standardization Organization
IT	Information Technology
ITS	Intelligent Transportation System
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
IVI	In-Vehicle Infotainment
NFC	Near Field Communication
OBD	On-Board Diagnostic
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over the Air
QMS	Quality Management System
SAE	Society of Automotive Engineers
SFS	Suomen Standardisoimisliitto ry
SUMS	Software Update Management System
TARA	Threat Analysis and Risk Assessment
TPM	Trusted Platform Module
UNECE	United Nations Economic Commission for Europe
VTA	Vehicle Type Approval
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
WiFi	Wireless network

1 INTRODUCTION

Technological advances in information and communication technologies (ICT) have resulted in unprecedented opportunities and innovation for improving farming outcomes. Agricultural equipment manufactures integrate computing and networking technologies creating cyber physical systems (CPS) such as smart farming, mobility services and connected vehicles. CPS-model offer communication capabilities anytime and anywhere.

1.1 Background for study

Agriculture is one of the oldest businesses that has undergone regular changes to level up with the population growth, market trends and technological innovations. It started with the use of the traditional way of farming. This means using hands and cattle to take care of the farms. Demand for large quantities of agricultural products increases as the population grows. To bridge the gap between the market's demand and supply, agricultural equipment manufacturers came into existence. Agricultural equipment manufacturers came up with an amazing line of products that ease the process of farming. These equipment can be employed for pushing/pulling the machinery that is used for ploughing, tilling, disking, harrowing, and planting. The ongoing demographic explosion and climate change are putting enormous pressure on world food production to feed 9.6 billion people by 2050 (United Nations, 2019). For this reason alone, there is a need to boost agriculture productivity in many ways.

Agriculture business has changed from single farm operations to agriculture industry. Over the centuries agriculture has been developed related to farming itself like from early days field farming to new innovations in crop production for example vertical farming, food production applications and services, and development of agricultural equipment's (Benke and Tomkins, 2017). Today agricultural businesses are stepping towards more modern versions of technology. Drivers for this are harvest optimization, growth of automation and digitalization (Ayaz et al., 2019). The digitalization in agriculture context refers to the use of sensors and other devices capabilities to turn every element and action involved in farming into data.

Smart agriculture will benefit from using Internet of Things (IoT) technology to farming operations data collection where sensors and smart devices are connected through Internet network (Gowda et al., 2021). In crop production, smart agriculture may be defined as tillage, sowing, irrigation, application of plant protection products and harvesting take place at exactly the right time, in the right place, with the right sizing and under favorable conditions. Sensors can be placed in the soil and environment to measure moisture and composition, even to monitor pests. Stocks can be monitored with meters and sensors: feed and grain silos, fertilizer and chemical depots, water tanks and stool tanks (Collin and Saarelainen, 2016). In the production itself, in addition to arable farming, the application areas are horticulture, greenhouse cultivation and control of livestock and pastures. According to research by Saiz-Rubio and Rovira-Más (2020) it is estimated that the implementation of IoT techniques has potential to boost agriculture 70% by 2050.

Autonomous work machinery, field and service robotics have been subjects of growing interest for many years in research and the mobile machine industry. Main interest for research has been to develop autonomous robotics concepts that will replace human operator of the machines. These technology solutions are applied also to agriculture machinery (Rondelli et al., 2022). Automatic vehicle guidance and steering control of agricultural machines takes care of driving the machine (Thomasson et al., 2019). In this way, the machine does overlap field from the same point many times, for example during seeding, spraying, fertilizing, and harvesting. It saves fuel, seeds, fertilizers, plant protection products and soil from unnecessary consumption and increases machine efficiency (Antille et al., 2018).

By sensing crop equipment, implements and tools, their use becomes more efficient and unexpected machine breakdowns are reduced (Gowda et al., 2021). The farmer can optimize equipment’s use, see the utilization rate and always know where the equipment is located (Antille et al., 2018). The equipment rental model will also be possible, for example rental based on operating hours. The farmer no longer needs to own everything that improves the balance sheet (Collin and Saarelainen, 2016).

Technology trends are changing traditional farming towards data-driven, farmer-centered, and knowledge-based smart farming. Data is collected from many data sources on the farm. This data can be combined with other data sources like data from, for example, weather services and satellite images. In the processed and analyzed form data is transformed to information that provides more value for the farmer and many other relevant parties (Ayaz et al., 2019). Smart farming is not intended to replace the farmer's experience and feel. Instead, the farmer will be able to make better quality conclusions with better and much more accurate information (Saiz-Rubio and Rovira-Más, 2020).

Ongoing technological changes affect significantly to traditional agricultural equipment manufacturers’ business. The business models of agricultural machinery manufacturers have transformed as they change from mere equipment suppliers to comprehensive service providers and equipment get cyber capabilities. For the first time, manufacturers will receive accurate information on the actual use of the sold equipment’s. At the same time, the customer relationship takes on a whole new dimension and all parties in the ecosystem benefit based on the new value that data can provide (Gowda et al., 2021).

1.2 Research motivation

Wireless networks of a connected vehicle provide new paths and methods, called attack vectors, for new types of cyberattacks compromising vehicle cybersecurity. It is complex to secure a connected vehicle from intrusions. Therefore cybersecurity is becoming a key issue with the main objectives of detecting, deterring, and averting vulnerabilities.

This work that has been done in automotive domain provides base for principles and processes for cybersecurity management that can be implemented also agricultural equipment manufacturers organizations who provide vehicles for offroad and public roads.

1.3 Research aims and scope

Cybersecurity is one of the cross-cutting issues in automotive ICT. Ongoing transformations in digitization enhance and create new paradigms when vehicle manufactures embed CPS such as connected vehicles and mobility services. Vehicle manufacturers must think about cybersecurity from an entirely new standpoint. Cybersecurity requires extensive internal transformation across vehicle manufacturers operations (Möller and Haas, 2019). According Möller and Haas (2019) cybersecurity is the body of technologies about processes, and practices designed to protect computers, data, networks, and programs against intrusion, damage, or unauthorized access by cyberattacks.

The high-level research aim of this thesis is to investigate cybersecurity and management processes of connected vehicles. This is quite a broad topic for research in one thesis. Three research questions are formed that narrow the research scope.

The first question can be written to analyze the current state of regulation. Governments and industry have independently published an array of principles, guidelines and proposed standards to support the automotive industry. These are usually open to interpretation and present complex challenges for vehicle manufacturers and the supply chain of the industry.

> Research Question 1: What is the status of automotive industry regulations and standards related to cybersecurity?

Cybersecurity in general perspective deals with risk management via risk quantification. Once a risk for an unauthorized intrusion has been identified, an analysis is carried out to determine the likelihood (probability) of the risk occurring and the consequence (impact) of that risk should it occur. This can be analyzed using a suitable method. The second question can be written to analyze risk.

> Research Question 2: How to manage cybersecurity risk of connected vehicles?

Regulations influences on organization work processes and management on many levels. The third question can be written to analyze changes in organization management.

> Research Question 3: How connected vehicles affect organization management related to product cybersecurity?

Scope of this thesis is limited to cybersecurity of connected vehicles, to explore and observe the cybersecurity phenomena related to governance aspects in vehicle manufacturer processes and to develop an evaluation tool of organizational cybersecurity capabilities related to cybersecurity of connected vehicles. Implementation methods of the processes and cybersecurity technologies are out of the scope of this thesis.

1.4 Research process and methodology

The theoretical foundation of the thesis is formed using research articles, reports, literature, and standards in the cybersecurity and automotive domains. The empirical part of the thesis is performed using design science methodology. A design science or design thinking approach is a suitable method for structured and collaborative development of new solutions, to create new knowledge about them and their usage (Schallmo, et al. 2018). Focus on design science research is problem solving and Venable and Baskerville (2012) have defined it as "research that invents a new purposeful artefact to address a generalized type of problem and evaluates its utility for solving problems of that type" (Venable and Baskerville, 2012 p. 142). Design science is suitable when a researcher builds a concrete, specific real-world subject.

In chapter 1, the context of the study has been introduced. The research objectives and questions have been identified and the value of such research argued. In chapter 2 essential perspectives to cyber are introduced and a review of existing literature is conducted forming the theoretical base. Through these two chapters, scientific research materials, such as peer-reviewed articles, literature, research reports, international standards, and publications from research institutes, are examined. Chapter 3 describes the implications of standards and regulations for vehicle manufacturers. Chapter 4 describes the empirical part of the thesis that is performed as design science research and develops evaluation tool for organizational cybersecurity management process capabilities. Chapter 5 provides a discussion of the research results in this thesis. Finally chapter 6 provides conclusions to performed research and sketches possible future work. The limitations of the study is also discussed.

1.5 Introduction to AGCO Corp

This master’s thesis is done in co-operation with and partly for AGCO corporation that is the third largest agricultural equipment manufacturer in the world. The company was established in 1990 and is headquartered in Duluth, Georgia, United States, and it is listed in NYSE stock market. The company has grown through the acquisition of agricultural companies as well as through organic growth. Net sales in 2022 were US $ 12,7 billion.

AGCO delivers sustainable high-tech solutions to farmers. It has been regularly interacting with its customers to bring out the best quality products, using the most advanced technology among the agricultural equipment manufacturers. AGCO machinery production provides full liner machinery solution to farmers: tractors, combine harvesters, and various agricultural equipment such as sprayers, hay, forage, and sugar cane harvesters. These agricultural equipment is sold under four main brands: Valtra, Massey Ferguson, Fendt and Challenger. AGCO also has its own engine manufacturing business AGCO Power. This business unit produces high quality engines for AGCO internal use in the company’s own machinery, external customers and the business unit own product that is a diesel engine powered electricity generator. AGCO's products are sold through its own sales network and independent dealers in more than 140 countries around the world.

2 LITERATURE REVIEW

The literature review provides different views on cyber phenomenon and its security aspects. The review also covers up to date regulations and standards of E/E (electrical and electronic) -systems for road vehicles manufacturers.

2.1 Key perspectives to cyber

2.1.1 Cyber and cyberspace

The word cyber is generally believed to originate from the Greek verb κυβερεω (kybereo) to steer, to guide and to control. At the end of the 1940s an American mathematician Norbert Wiener (1894 – 1964) began to use the word cybernetics to describe computerized control systems. According to Wiener, cybernetics deals with sciences that address the control of machines and living organisms through communication and feedback (Lehto, 2015).

There are many terms and concepts that are associated to provide definition for cyberspace phenomenon. The International Organization for Standardization (ISO) defines cyberspace in ISO15408 standard as complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form (ISO/IEC 15408, 2009). Lehto (2018) has defined cyberspace that it is a man-made ecosystem. While land, air, sea and space domains exist without any human presence, cyberspace requires continuous human attendance and activities (Lehto, 2018).

Merriam Webster online dictionary provides simple definition “Cyberspace is the online world of computer networks and especially the Internet” (Merriam-Webster, 2022). And the Internet has been considered as the real-life implementation of cyberspace. But according to Lehto (2018) cyberspace is more than the just internet. It includes not only hardware, software, data and information systems, but also people and social interaction within these networks and the whole infrastructure. CPS is a new generation of digital systems. It composed of physical system components, computational and cyber capabilities that have a very tight interconnectivity (Kure et al., 2018).

2.1.2 Cyberspace taxonomy and asset

Research by Inglis (2016) has provided reference framework model describing taxonomy in cyberspace by studying center point which not only is the result of integrating diverse technologies and human actions, but which also serves as a resource enabling widespread collaboration and integration. Taxonomy allows focused discussions about discrete aspects of cyberspace and their relationship to each other (Inglis, 2016). Figure 1 illustrates Inglis' taxonomy reference model.

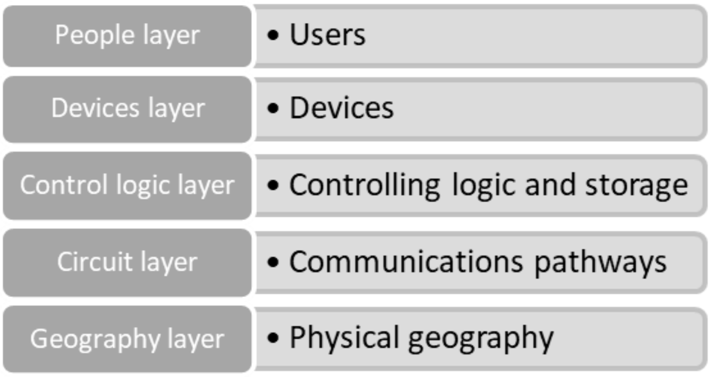

Figure 1. Cyberspace reference model: a mix of geography, technology, and people (modified from Inglis 2016)

Assets are either information or business processes considered valuable by an organization, including buildings, equipment, personnel, organization reputation, business documents and other tangible and intangible assets (ISO 27002, 2018). Information asset is "any collection, set, or database of information or any asset that collects, stores, processes, or transmits information of value to the organization" (Whitman and Mattord, 2019 p. 319).

2.1.3 Vulnerability, threat and risk

ISO standardization organization has defined vulnerability as a weakness of an asset or control that can be exploited by one or more threats (ISO 27002, 2018). In the system view vulnerability is a weakness in a system that may be exploited to degrade or bypass system standard security mechanisms (Andress, 2014). According to Lehto (2018) vulnerabilities can be divided into those that exist in human action, processes, or technologies. For example, if a system does not have antivirus software, that would compose a vulnerability.

A threat can be anything that is trying to downgrade, disrupt or steal your asset (Bokan and Santos, 2021). The ISO standard defines threat as a potential cause of an unwanted incident, which may result in harm to a system or organization (ISO 27002, 2018). The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets. The numeric value of the threat represents its degree of probability (Lehto, 2018). For example, the existence of a particular virus represents a threat to a system.

According to Kure et al. (2018) risk can be defined as an uncertain event that may occur due to a system malfunction or failure that could harm assets, such as human beings or the environment, and influence the organization’s achievement on strategic, operational, and financial objectives. A risk occurs when a threat and a corresponding vulnerability both exist (Solomon and Chapple, 2005). Risk arises from the possibility that a threat may exploit a vulnerability to breach security and cause harm to an asset – in worst case the asset’s total loss (Bokan and Santos, 2021). Figure 2 illustrates the relationship between threats, risks, and vulnerabilities in the Venn diagram.

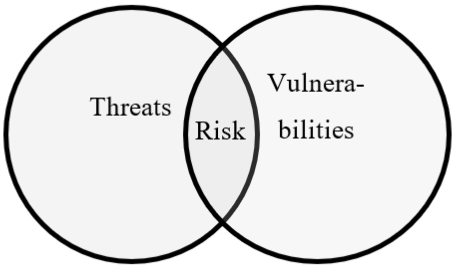

Figure 2. The relationship between threats risks and vulnerabilities (based on Solomon & Chapple 2005)

For example, the vulnerability of a system combined with the threat of a harmful virus without antivirus software combines to constitute a risk to that system.

2.1.4 CIA and DAD triads

Information security profession, practitioners tend to describe information security as the sum of its fundamental attributes: Confidentiality, Integrity, and Availability. This is known as the CIA-triad. These are the three requirements that users demand from information systems, and they are the cornerstones of any well-designed information security program (Solomon and Chapple, 2005). There exist also other models that have common attributes of the CIA-triad (Andress, 2014). Figure 3 illustrates the CIA triad relation to information security.

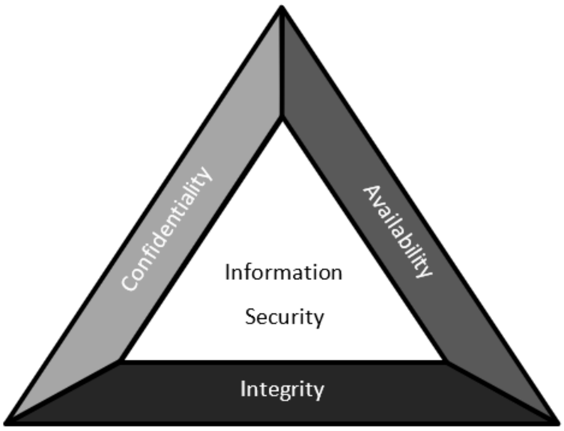

Figure 3. CIA triad relation to information security (based on Solomon & Chapple, 2005)

Primary goals of the CIA attributes can be defined as following:

- **Confidentiality** goal of information security programs prevents unauthorized personnel use of confidential information. Only selected users can access to specific data.
- **Integrity** basic goal is ensuring that data may be modified only through an authorized mechanism. Integrity involves protecting data from all kinds of unauthorized modification.
- **Availability** goal is to guarantee the ability of authorized users to uninterrupted access information, systems and networks (Solomon and Chapple 2005).

There are three primary mechanisms that are used by malicious individuals to defeat these three information security properties: disclosure, alteration, and denial. The model is known as DAD-triad (Solomon and Chapple, 2005). An illustration in Figure 4 shows how DAD triad components relate the CIA triad.

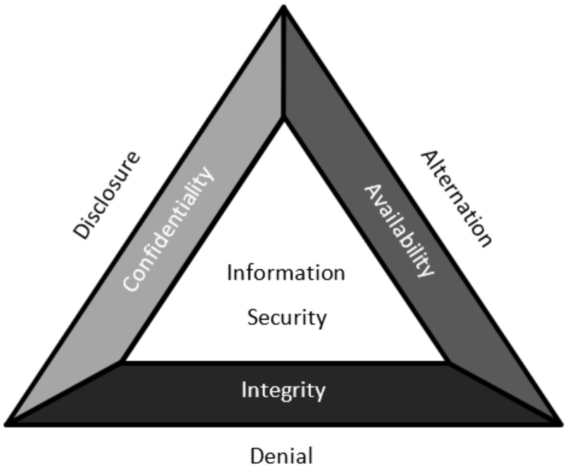

Figure 4. DAD relation to CIA triad (based on Solomon & Chapple, 2005)

Disclosure occurs when unauthorized individuals gain access to confidential information. It occurs when security professionals fail, in one way or another, to achieve the CIA triad's goal of confidentiality. Data alteration occurs when security mechanisms tail to ensure the integrity of data. Unauthorized alteration can be the result of either malicious or accidental activity. Denial occurs when events take place that prevent authorized users from accessing a system for legitimate reasons (Solomon and Chapple, 2005).

2.2 Risk management, cybersecurity and connected vehicles model

Risk management is a continuous process of an organization to respond uncertainty that can impact to the outcomes of their operations. Hopkin (2018, p.44) has defined risk management "As the set of activities within an organization undertaken to deliver the most favorable outcome and reduce the volatility or variability of that outcome" (Hopkin, 2018). The risk management process can be divided into several steps. Risk identification is the process of identifying and assessing threats to an organization, its operations and its workforce. Risk analysis involves establishing the probability that a risk event might occur and the potential outcome of each event. A risk assessment is a process to identify potential hazards and analyze what can happen if a hazard occurs (Aven, 2016). Risk treatment is the process of selecting and implementing measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk (Hopkin, 2018).

2.2.1 Cybersecurity

Möller and Haas (2019, p. 265) have provided a comprehensive description for cybersecurity. “In general cybersecurity is the body of technologies about processes, and practices designed to protect computers, data, networks, and programs against intrusion, damage, or unauthorized access by cyberattack” (Möller and Haas, 2019).

According to Särkkä (2021) organizational approach to cybersecurity may be divided to four categories. Passive, it is hoped and imagined that cyber security does not apply to one's own company, the company's management is not interested in security. Reactive, cybersecurity is outsourced to IT department and risks are handled when occurred. Proactive, management of the company actively seeks to take measures to improve security and prepare for future threats. Progressive, the organization understands that it is a constant target and is aware of the possibility of failure. Control effectiveness is measured and audited, and efforts are made to reduce the impact of potential data lost (Tekniikka & Talous, 2021).

2.2.2 Connected vehicles model

European Union Agency for Cybersecurity (ENISA) has formulated the high-level functional model of connected vehicle and its connection to Intelligent Transportation System (ITS) (European Union Agency for Cybersecurity, 2019). ITS are advanced applications which aims to provide innovative services relating to different modes of transport and traffic management and enable users to be better informed and make safer, more coordinated, and 'smarter' use of transport networks (Mahmood et al., 2022). Illustrated model in Figure 5 is only informative reference and it doesn’t reflect complexity of various automotive architectures.

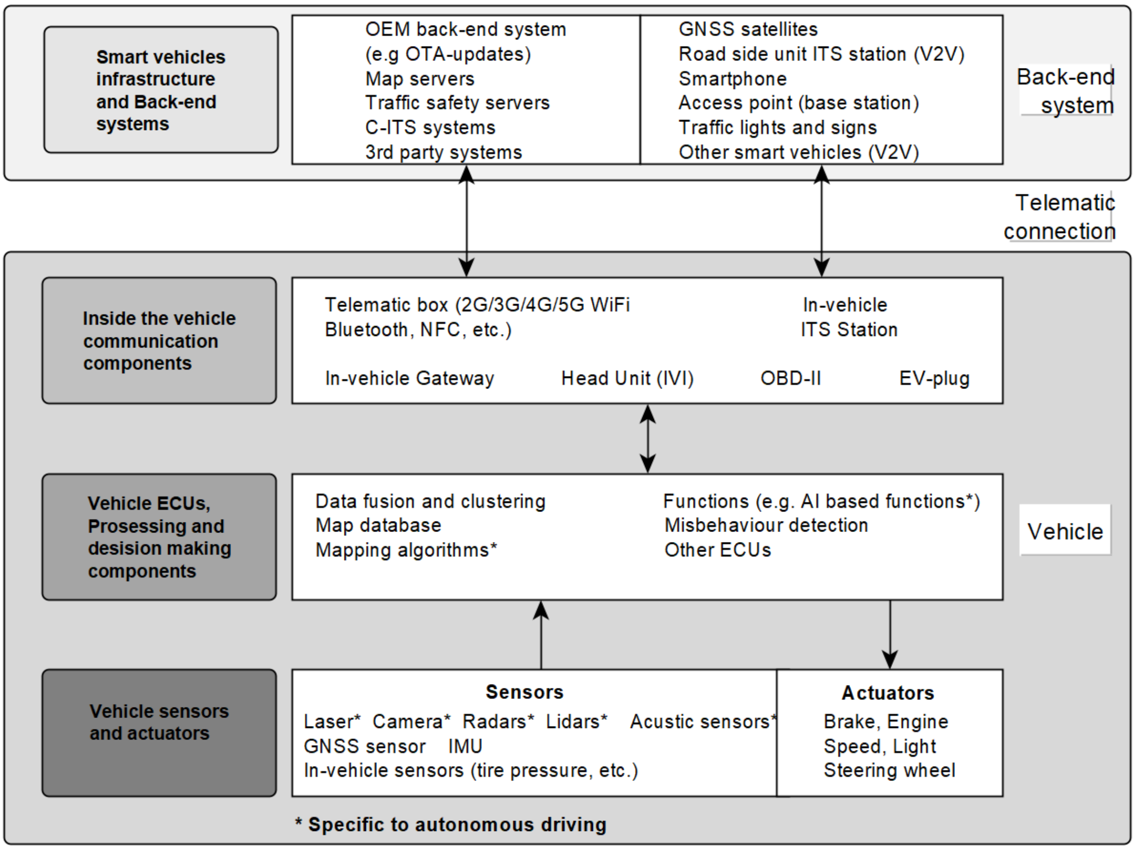
Smart vehicles infrastructure and Back-end systems
OEM back-end system
(e.g OTA-updates)
Map servers
Traffic safety servers
C-ITS systems
3rd party systems
GNSS satellites
Road side unit ITS station (V2V)
Smartphone
Access point (base station)
Traffic lights and signs
Other smart vehicles (V2V)
Back-end system
Telematic connection
Inside the vehicle communication components
Telematic box (2G/3G/4G/5G WiFi Bluetooth, NFC, etc.)
In-vehicle ITS Station
In-vehicle Gateway
Head Unit (IVI)
OBD-II
EV-plug
Vehicle ECUs, Prosessing and desision making components
Data fusion and clustering
Map database
Mapping algorithms*
Functions (e.g. AI based functions*)
Misbehaviour detection
Other ECUs
Vehicle
Vehicle sensors and actuators
Sensors
Laser* Camera* Radars* Lidars* Acustic sensors*
GNSS sensor IMU
In-vehicle sensors (tire pressure, etc.)
Actuators
Brake, Engine
Speed, Light
Steering wheel
* Specific to autonomous driving

Figure 5. Functional model of connected vehicle (modified from ENISA 2019)

The model describes three layers that relate to ITS system: backend system, telematic connection and vehicle. According to the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) definition Intelligent Transport System (ITS) -system including autonomous driving system, provides various kind of applications and services to increase safety on road, mitigate the environmental footprint of transport, enhance traffic management and maximize the transport sector’s benefits to public and commercial users” (ITU-T, 2022).

2.3 Laws, automotive cybersecurity regulations and standards

Varied definitions may often confuse differences between laws, regulations, and standards. Generally, it is possible to define that legislative bodies pass laws, government agencies develop regulations to implement the laws. Laws are the system of rules made by the government of a country and needs to be signed by high authority like president or governor. Regulations are instructions provided by regulatory bodies or public authorities how laws are to be carried out or enforced (Bronwen and Karen, 2007).

According to the University of Massachusetts Amherst definition standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose (University of Massachusetts Amherst, 2022). Standardization organizations develop standards on three levels. First, international standards are developed by International Standardization Organization (ISO), International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) for adapting to national use. Second, regional standards are developed for specific region like European Union’s European Telecommunications Standards Institute (ETSI), European Committee for Electrotechnical Standardization (CENLEC) and European Committee for Standardization (CEN) standards or North America’s Society of Automotive Engineers (SAE) and American National Standards Institute (ANSI) standards. Third, national standards are developed either by a national standards body, like Suomen Standardisoimisliitto (SFS) in Finland, Deutsches Institut für Normung (DIN) in Germany, or some other accredited bodies.

Compliance with the standard often means compliance with the relevant legislation. However, there are usually some other ways to achieve compliance with legislation without using a standard (British Standards Institution, 2022).

2.3.1 Functional safety and cybersecurity

Functional safety and cybersecurity engineering are closely related disciplines in automotive engineering. Both of these disciplines focus engineering system-wide features. When adequate interactions between their processes are defined, functional safety and cybersecurity engineering can greatly benefit from each other (Schmittner and Macher, 2019). Functional safety answers the question that does the vehicle function as it should and is everything as safe as possible. Functional safety is about ensuring only desired processes while reducing the risk of unintended hazards as much as possible for example malfunctions. Cybersecurity engineering answers to the question that how everything can be secured to such an extent that risks can be managed as well as possible (Zayane, 2022).

2.3.2 Functional safety regulations and standards for vehicle engineering

Functional safety engineering is already part of today’s automotive engineering. Safety standards are integrated well to automotive products’ development process (Schmittner and Macher, 2019). Table 1 describes the key functional standards for engineering.

Table 1. Functional safety standards

Document	Description	Status
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)	Published 2010
ISO 26262	Road vehicles — Functional safety	Published 2018
ISO 25119	Tractors and machinery for agriculture and forestry – Safety-related parts of control systems	Published 2018

IEC 61508 is an international standard for functional safety consisting of general methods on how to apply, design, deploy and maintain electrical, electronic and programmable electronic safety related systems. Standard is titled “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)” (IEC 61508, 2010).

ISO 26262 titled “Road vehicles - Functional safety” standard is a sector specific implementation of IEC 61508 for Automotive Electric and Electronic systems. Edition 2.0 was published 2018 and it includes interaction recommendations with safety and security (ISO 26262, 2018).

ISO 25119, titled "Tractors and machinery for agriculture and forestry – Safety-related parts of control systems”. The standard is a sector specific implementation of IEC 61508 for functional safety of electrical and electronic systems that are installed in tractors and machines used in agriculture and forestry (ISO 25119, 2018).

2.3.3 United Nations regulation for new vehicle type approval

The United Nations Economic Commission for Europe (UNECE) represents one of the five regional commissions under the jurisdiction of the United Nations Economic and Social Council. UNECE is composed of more than 60 states that, some of which are also members of UNECE WP.29. The UNECE WP.29 World Forum for Harmonization of Vehicle Regulations is a unique worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee (UNECE, 2022).

In March 2021 UNECE WP.29 members published new regulations for cybersecurity in road vehicles. Within the UNECE WP.29 regulations, two documents cover key future topics in the automotive domain: Cybersecurity R155 (UNECE, 2021a) and Software Update R156 (UNECE, 2021b). The regulations include making efforts to manage risks, detecting and responding to cybersecurity threats, designing secure systems across the supply chain, and providing secure software updates for on-board systems for the lifetime of the vehicle.

UNECE WP.29/R155 regulation titled "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system" does not determine car manufacturers how to secure their vehicles, but it outlines management actions that have to be taken. The regulation consists of the requirement to implement Cyber Security Management System (CSMS) that is defined as "systematic risk-based approach defining organizational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks" (UNECE, 2021a).

In UNECE states it is mandatory for vehicle manufacturers and suppliers to meet WP29 regulations for all new vehicle types to homologate new vehicle types as on 6th July 2022 and it will become mandatory for all vehicles produced types from July 2024 (Costantino et al., 2022).

2.3.4 ISO/SAE 21434 cybersecurity engineering standard for road vehicles

ISO/SAE 21434 standard for automotive cybersecurity engineering is an outcome of work done by two organizations experts: SAE International and ISO. The structure of the standard is illustrated in Figure 6. Standard focuses on automotive cybersecurity engineering framework for road vehicles. It provides requirements for management and engineering processes of the E/E -systems from the cybersecurity perspective for vehicles, including the participants in the supply chain. Standard also specifies requirements and provides recommendations for cybersecurity risk management for cars throughout their entire lifecycle including their components, software and interfaces (ISO/SAE 21434, 2021).

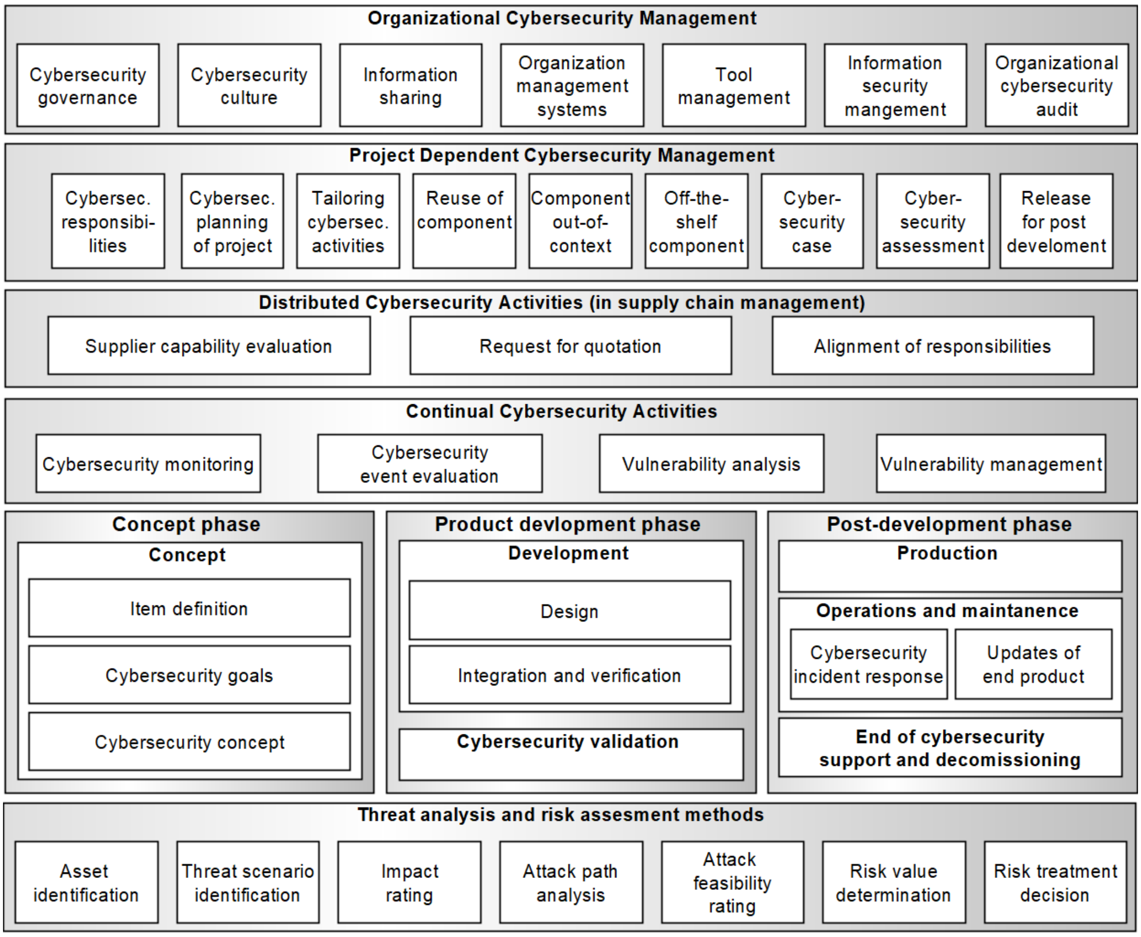
Organizational Cybersecurity Management
Cybersecurity governance
Cybersecurity culture
Information sharing
Organization management systems
Tool management
Information security mangement
Organizational cybersecurity audit
Project Dependent Cybersecurity Management
Cybersec. responsibi-lities
Cybersec. planning of project
Tailoring cybersec. activities
Reuse of component
Component out-of-context
Off-the-shelf component
Cyber-security case
Cyber-security assessment
Release for post develoment
Distributed Cybersecurity Activities (in supply chain management)
Supplier capability evaluation
Request for quotation
Alignment of responsibilities
Continual Cybersecurity Activities
Cybersecurity monitoring
Cybersecurity event evaluation
Vulnerability analysis
Vulnerability management
Concept phase
Concept
Item definition
Cybersecurity goals
Cybersecurity concept
Product devlopment phase
Development
Design
Integration and verification
Cybersecurity validation
Post-development phase
Production
Operations and maintanence
Cybersecurity incident response
Updates of end product
End of cybersecurity support and decomissioning
Threat analysis and risk assesment methods
Asset identification
Threat scenario identification
Impact rating
Attack path analysis
Attack feasibility rating
Risk value determination
Risk treatment decision

Figure 6. Overview of the ISO/SAE 21434-chapters structure (according to ISO/SAE 21434)

ISO/SAE 21434 standard pursues several objectives for the automotive industry. These objectives are:

- create a uniform terminology for cybersecurity engineering

- define minimum requirements for processes and activities in cybersecurity engineering
- promote cooperation between the parties involved in the value chain
- describe the “state of the art” of cybersecurity engineering

The purpose of ISO/SAE 21434 is applied to vehicles and their subsystems, components, connections and data. The aim is to establish a structured process for all participants in the value-added process and to firmly anchor the topic of security in the design process (ISO/SAE, 21434 2021; Marty, 2021). Motivated by the goal of establishing “security by design“, the security risk analysis fulfills a special role in ISO/SAE 21434 by determining security risk levels for the entire vehicle and its individual components. The manufacturer has to prove that appropriate risk levels are achieved (Hornbogen, 2020). The standard does not provide concrete solutions to implementation approaches for different technologies like network or encryption technologies.

2.3.5 SAE cybersecurity standardization activities

The SAE Vehicle Electrical System Security Committee developed the first cybersecurity SAE J3061 guideline dedicated to automotive sector. The guideline establishes a set of high-level guiding principles for cybersecurity:

- defining a complete lifecycle process framework
- providing information on some common existing tools and methods
- supporting basic guiding principles on cybersecurity
- summarizing further standard development activities

After this development work SAE has published several other standards in the area of automotive cybersecurity. Table 2 describes the standards developed by SAE and their status.

Table 2. SAE standards and their development status

Document	Description	Status
SAE J3101	Define implementation requirements for hardware protected security for ground vehicles	Published 2020-2-1
SAE J3138	Diagnostic Link Connector Security	Published 2018-06-02
SAE J3061_202112	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	Published 2021-12-15
SAE J3061-2	Security Testing Methods	Work in Process
SAE J3254	Automotive Cybersecurity Maturity Model Best Practice	Work in Process
SAE J1939-91A-C	Network Security in J1939 controller area networks	Work in Process

New release of **SAE J3061:2021** recommended practices. It provides guidance on vehicle cybersecurity. The standard was created based on SAE J3061:2016 and expanded from existing practices which are being implemented or reported in industry, government, and conference papers. The appendices provide additional information to be aware of and can be used in improving feature designs cybersecurity (SAE J3061_202112, 2021).

SAE J3061-2 Security Testing Methods. Overview of currently available software and hardware security testing methods.

SAE J3101 Hardware Protected Security for Ground Vehicle **-**standard document aims to define common requirements to be implemented in hardware-assisted functions to facilitate security-enhanced applications, to achieve an ideal system for hardware protection for ground vehicle applications (SAE J3101, 2020).

SAE J3138 Diagnostic Link Connector Security -document describes some of the actions that should be taken to help ensure safe vehicle operation in the case that any such connected device (external test equipment, connected data collection device) has been compromised by a source external to the vehicle (SAE J3138, 2018).

SAE J3254 The intent of this standard document is to provide organizations guidance on how to define maturity and gauge cybersecurity posture in the automotive space. This document will outline the common maturity matrix applicable to the industry along with best practice activities. In the future this document can be used by organizations to develop self-certification to ISO 21434 in order to indicate progress and areas for improvement (SAE J3254, 2023).

SAE J1939-91A-C provides recommendations to vehicle manufacturers to protect controller area network from cybersecurity risks. Part A defines the recommendations for security of the vehicle side of the diagnostic interface connector. Part B defines recommendations for bi-directional Over The Air (OTA) communications security via a telematics interface to the vehicle. Part C defines recommendations for secure on-board communications between ECUs in CAN FD network.

2.3.6 ITU-T Intelligent Transport System (ITS) security

ITU is an international standardization organization for communication networks. ITU-T is Telecommunication Standardization Sector that develops international standards known as ITU-T Recommendations. Study group 17 provided several security recommendations for Intelligent Transport System (ITS). ITU efforts for the standards development and their development status are described in Table 3.

Table 3. ITU standards and their development status

Document	Description	Status
X.1372	Security guidelines for Vehicle-to-Everything (V2X) communication	Approved 2020-03-26
X.1373	Secure software update capability for intelligent transportation system communication devices	Approved 2017-03-30
X.1374	Security requirements for external interfaces and devices with vehicle access capability.	Approved 2020-10-29
X.1375	Guidelines for intrusion detection system for in-vehicle networks.	Approved 2020-10-29
X.1381	Security guidelines for the Ethernet-based in-vehicle networks	Under Study
X.itssec-5	Security guidelines for vehicular edge computing	Under Study

ITU-T X.1372 *Security guidelines for Vehicle-to-Everything (V2X) communication* - recommendation provides security guidelines for Vehicle-to-Everything (V2X) communication systems. V2X is a generic term for the communication modes termed as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-nomadic devices (V2D) and vehicle-to-pedestrian (V2P) discussed in this recommendation (ITU X.1372, 2020).

ITU-T X.1373 *Secure software update capability for intelligent transportation system communication devices* -recommendation provides secure software update procedures between a software update server and vehicles with appropriate security controls. This recommendation can be practically utilized by car manufacturers and ITS-related industries as a set of standard capabilities for best practices (ITU X.1373, 2017).

ITU-T X.1374 *Security requirements for external interfaces and devices with vehicle access capability* - recommendation analyzes security threats to connected vehicles in two parts. First threats against interfaces which are used to communicate between a vehicle and its external devices, and second, threats against external devices which communicate with the vehicle. This recommendation specifies security requirements for such external interfaces and external devices with vehicle access capability in telecommunication network environments to address identified threats depending on types of access interfaces. Interfaces and external devices with vehicle access capability include remote keyless entry (RKE) system with smart key, diagnostic tool and wireless dongle using on-board diagnostic II (OBD-II) port, telematics control units with wireless communication devices and so on (ITU X.1374, 2020).

ITU-T X.1375 *Guidelines for intrusion detection systems (IDSs) for in-vehicle networks* -recommendation focuses on how to detect intrusion and malicious activities on in-vehicle networks such as those using controller area network (CAN) that cannot be supported by general IDSs currently used in Internet deployments. This recommendation includes classifications and analyses of attacks targeting in-vehicle networks.(ITU X.1375, 2020)

ITU-T X.itssec-5 *Security guidelines for vehicular edge computing* - is ongoing ITU-T work program. This recommendation provides security guidelines for vehicular edge computing. Vehicular edge computing (VEC) is a model that supports the core cloud's capacity for decentralizing the concentration of computing resources in data centers. (ITU X.itssec-5, 2021)

ITU-T X.1381 *Security guidelines for the Ethernet-based in-vehicle networks* - is another ITU-T work program. Recommendation provides security guidelines for the Ethernet-based in-vehicle networks technology. The recommendation includes a reference model of automotive Ethernet and an analysis of threat and vulnerability for the Ethernet-based in-vehicle networks. In addition, recommendation provides the security requirements and use cases of the Ethernet-based in-vehicle networks (ITU X.1381, 2021).

2.3.7 ISO standardization activities

Also ISO has been developing standardization on specific automotive cybersecurity-related topics. The Table 4 describes outcomes of this work. ISO has developed the Extended Vehicle (ExVe) concept for accessing vehicle data and its interfaces. The extended vehicle concept consists of a physical road vehicle with external software and hardware extensions that are developed, implemented and managed by the vehicle manufacturer. ISO has developed these standards to ensure interoperability across the globe.

Table 4. ISO standards and their development status

Document	Description	Status
ISO 20077	Road Vehicles – Extended vehicle (ExVe) methodology	Published
ISO/DTS 20077-3	Extended vehicle (ExVe) methodology – Part 3: Upstream process to develop services	Work in process
ISO20078	Road vehicles – Extended vehicle (ExVe) web services – Part 1-4	Published, 2nd edition 2021
ISO/TR 23791:2019	Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078 series	Published
ISO 23132:2020	Road vehicles – Extended Vehicle (ExVe) time critical applications – General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)	Published

ISO 20077 *Road Vehicles – Extended vehicle (ExVe) methodology – Part 1-2*, Part 1 defines concepts and terms and presents general information regarding these vehicles. Part 2 specifies general rules and basic principles the manufacturer of the extended vehicle (ExVe) and considers when the manufacturer must elaborate its own design method (ISO 20077, 2017).

ISO/DTS 20077-3 *Extended vehicle (ExVe) methodology – Part 3: Upstream process to develop services*, describes the process to initiate and facilitate the communication between independent stakeholders and vehicle manufacturers.

ISO 20078:2021 *Road vehicles – Extended vehicle (ExVe) web services – Part 1-4:* Sets the recommendations for extended vehicle web services (ISO 20078:2021, 2021).

ISO/TR 23791:2019 *Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078 series*, presents the assessment of the safety, security, competition, responsibilities, and data protection risks that can originate from the ISO 20078 series (ISO/TR 23791:2019, 2019).

ISO 23132:2020 *Road vehicles – Extended Vehicle (ExVe) time critical applications - General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS),* defines the classification methodology of time-constrained situations and their requirements, that are to be addressed by the "ExVe time critical interfaces" described in ISO 20077-1(ISO 23132:2020, 2020).

2.3.8 Other relevant standards

There are also other standards for example, the IEC 62443 and ISO 27000 – series that are not developed for automotive systems engineering but are becoming ever more critical for cloud-connected service infrastructure (Dobaj et al., 2021). These international standard series are relevant for automotive industry to be used in organization IT infrastructure, back-end systems and production operational technology (OT). Operational technology can be defined as all network technology that controls production process and equipment. The Figure 7 describes relation of these standards to organization network systems.

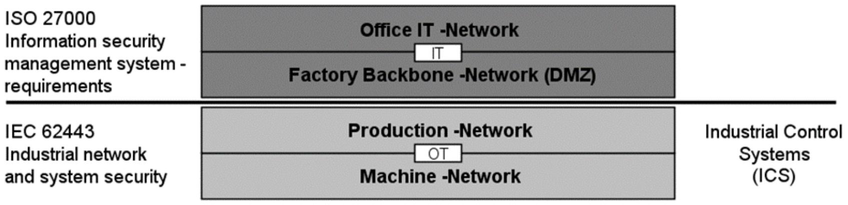

Figure 7. Standards for IT -infrastructure and industrial control systems

ISO 27000 Information technology - security techniques – series' standard provide best practice recommendations on information security management within the context of an overall Information Security Management System (ISMS). Including the management of information risks through information security controls (ISO 27000 series, 2018).

IEC 62443 *Industrial communication networks and system security* - is an international series of standards that address cybersecurity for operational technology (OT) in production automation and industrial control systems (ICS) (IEC 62443 series, n.d.).

3 IMPLICATIONS TO VEHICLE MANUFACTURERS

The following section describes implications of regulations and standards for vehicle manufacturers. More specifically, implications to organizational practices and engineering of E/E -systems within road vehicles.

3.1 Vehicle manufacturer cybersecurity organizational process

Cybersecurity has become one of the most important aspects in the automotive products' lifecycle. United Nations regulation UNECE WP.29/R155 on cybersecurity defines a set of requirements that needs to be fulfilled by vehicle manufacturers, suppliers and service providers, covering the entire vehicle lifecycle from the vehicle development to its decommissioning (UNECE, 2021a). The European Union wants to be the pioneer in the field of fully driverless vehicles. The European Commission has set new rules in the Vehicle General Safety Regulation (GSR) to improve road safety (European Parliament Council of the European Union, 2019). GSR establishes the legal framework for the approval of automated and fully driverless vehicles in the EU.

The GSR rules will first apply to new vehicle types: they have to fulfill for claiming for new type approvals as of June 2022 and to all new vehicles as of 7th July 2024. Some of the new measures will be expanded to cover different kinds of road vehicles by 2029 (European Parliament Council of the European Union, 2019). The evolution of smart vehicles' security takes major step when the vehicle manufacturers implement the GSR rules to their management practices.

3.1.1 GSR organizational cybersecurity management

GSR set new requirements for management systems and cybersecurity measures that vehicle manufacturers have to implement. This responsible vehicle manufacturer in the process is named as Original Equipment Manufacturer (OEM). UNECE WP.29/R155 and ISO/SAE 21434 standard are essential steps toward integrating cybersecurity in automotive management practices.

UNECE WP.29/R155 requires that OEMs have cybersecurity process framework implemented. This framework is called Cyber Security Management System (CSMS). ISO/SAE 21434 standard's purpose is to provide guidelines for CSMS implementation to organizational management practices including cybersecurity risk management (ISO/SAE 21434, 2021). ISO/SAE 21434 standard itself provides just a generic framework. The standard addresses the cybersecurity perspective in engineering. It provides requirements for management and engineering processes of the E/E -systems from the cybersecurity perspective for vehicles, including the participants in the supply chain. Standard requirements define a basis for the company-specific processes and practices development. The Figure 8 describes the relation between UNECE WP.29/R155 and ISO/SAE 21434 standard cybersecurity management processes.

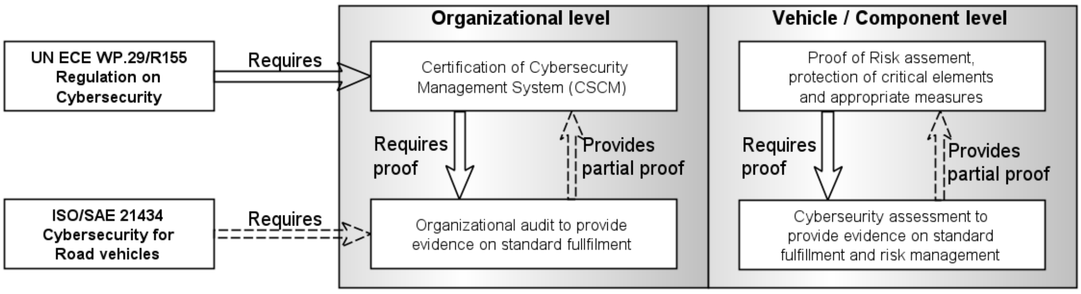
Organizational level
Vehicle / Component level
UN ECE WP.29/R155 Regulation on Cybersecurity
Requires
Certification of Cybersecurity Management System (CSCM)
Proof of Risk assement, protection of critical elements and appropriate measures
Requires proof
Provides partial proof
Requires proof
Provides partial proof
ISO/SAE 21434 Cybersecurity for Road vehicles
Requires
Organizational audit to provide evidence on standard fullfilment
Cyberseurity assessment to provide evidence on standard fulfillment and risk management

Figure 8. UNECE WP.29/R155 relation ISO/SAE 21434

According to UNECE WP.29/R155, vehicle manufactures must take three steps approach to get an approval for a new vehicle type (UNECE, 2021a). Figure 9 illustrates relation of all three steps and process activities.

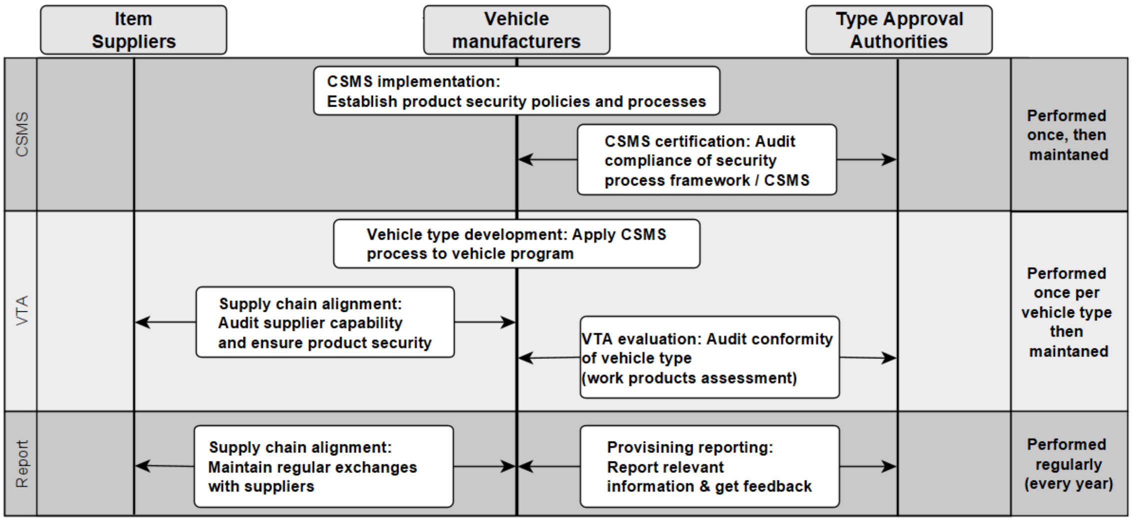
Item Suppliers
Vehicle manufacturers
Type Approval Authorities
CSMS
VTA
Report
CSMS implementation: Establish product security policies and processes
CSMS certification: Audit compliance of security process framework / CSMS
Performed once, then maintaned
Vehicle type development: Apply CSMS process to vehicle program
Supply chain alignment: Audit supplier capability and ensure product security
VTA evaluation: Audit conformity of vehicle type (work products assessment)
Performed once per vehicle type then maintaned
Supply chain alignment: Maintain regular exchanges with suppliers
Provisining reporting: Report relevant information & get feedback
Performed regularly (every year)

Figure 9. GSR implications to organizational processes (modified from Marty 2021)

First, UNECE WP.29/R155 requires that vehicle manufacturers must demonstrate to authorities their implementation of CSMS. It is mandatory to have the CSMS audited by authorities and get a CSMS certificate to prove that a vehicle manufacturer has organizational capability to fulfill the requirements (UNECE, 2021a).

Second, when CSMS is certified by the authority, a vehicle manufacturer has the right to apply for Vehicle Type Approvals (VTA). During this phase the manufacturer must demonstrate to the authorities the real implementation of processes described within the CSMS for this specific vehicle type program or specific vehicle. The objective of the second step is to evaluate that certified cybersecurity process framework has been successfully implemented. In this phase it is necessary to provide documentation that demonstrates vehicle security processes implementation for example for risk assessment process. This documentation provides evidence of complete risk assessment details for this specific vehicle type.

The third step is to maintain authorization. Even though the VTA for a vehicle has been authorized, the manufacturer must maintain the authorization in order to continue selling the vehicle on the market. Manufacturers have to regularly (once a year) provide provision report for authorities (UNECE, 2021a). The main objective of this reporting is to demonstrate to the authorities that protection measures are still effective and adequate against evolving threat landscape. This report is the outcome of the manufacturer's cybersecurity monitoring activities, information related to new cyber-attacks and potential incidents that may require adjustment of cybersecurity measures. The process for continual cybersecurity activities is defined in ISO/SAE 21434 standard.

3.1.2 Supply chain management

The UNECE WP.29/R155 regulation defines new rules only to vehicle manufacturers via homologation authorities (UNECE, 2021a). Some of those rules address security aspects across OEMs' full supply chain. Supply chains can be broken down into a system of "Tier 1-3" based on closeness to OEMs business or final product. A Tier 1 supplier is a company that is a direct supplier for an OEM. The simple definition for Tier 2 supplier is the company that provides components for Tier 1 supplier. Finally, Tier 3 supplier is one step further from a final product and typically provides parts or work with raw materials for Tier 2 suppliers.

The UNECE WP.29/R155 regulation has significant influence on every supplier that provides security critical elements to OEMs. It is OEM's responsibility to derive relevant requirements for their own suppliers to collect enough evidence for proving supplier capabilities to develop, operate and maintain the security of supplied elements. The Figure 10 illustrates OEM's responsibilities to supply chain and approval authority.

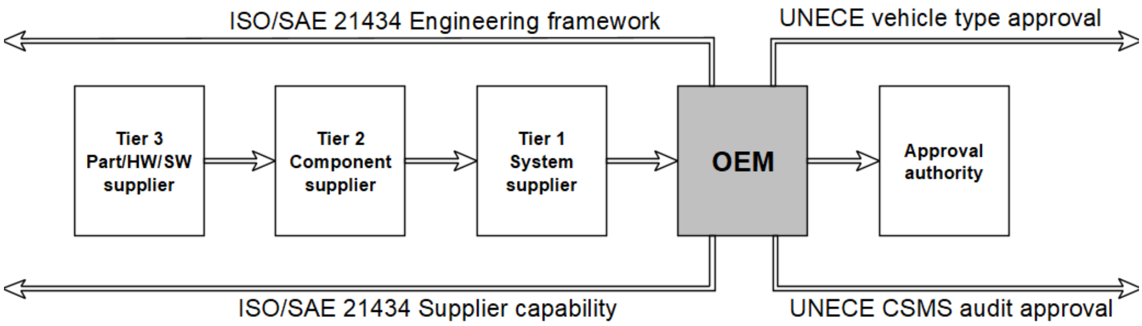
ISO/SAE 21434 Engineering framework
UNECE vehicle type approval
Tier 3 Part/HW/SW supplier
Tier 2 Component supplier
Tier 1 System supplier
OEM
Approval authority
ISO/SAE 21434 Supplier capability
UNECE CSMS audit approval

Figure 10. OEMs two side cooperation and their dimensions to requirements (modified from Marty, 2021)

ISO/SAE 21434 standard defines requirements of distribute cybersecurity activities to OEMs suppliers:

- define relevant cybersecurity requirements to be distributed to their suppliers for ensuring end-to-end security across the supply chain

- responsibility for qualifying and approving suppliers for providing security compliant products and services
- responsibility for securing the alignment of shared activities with suppliers (interface agreements)

UNECE WP.29/R155 regulation defines OEMs' obligations towards authorities:

- demonstrate evidence to authorities of CSMS implementation
- demonstrate vehicle type specific evidence proving reasonable mitigation measures for cyber risks

3.2 Functional safety and cybersecurity risks

Functional safety and cybersecurity are independent disciplines, and both deal with risk management methods and processes. The purpose of these processes and methods is to guarantee absence of unreasonable risk due to hazards caused by malfunctioning behavior or compromised security. Impacts of the hazards have to be considered from the road user's perspective, not the corporate's perspective. The Figure 11 illustrates fundamental assessment-related differences and why specific approaches are required.

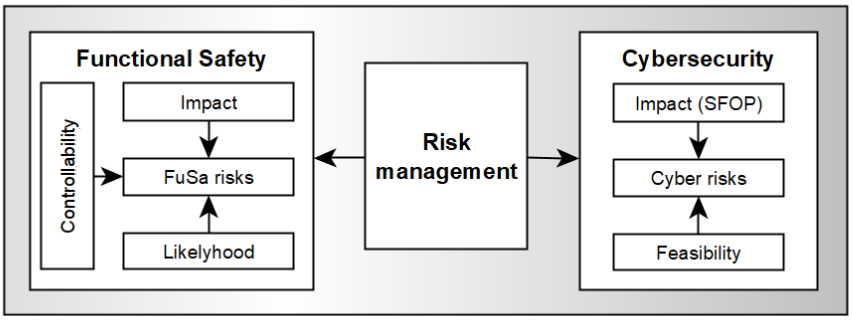

Figure 11. Risk management landscape differences (based on Marty, 2021)

The typical functional safety risk assessment approach for automotive domain is evaluating potential damage based on three key factors: safety impact/severity, likelihood/exposure and controllability of an adverse event. The cybersecurity approach is different. In general, cybersecurity deals with risk management via risk quantification. A typical approach to rate the impact is to evaluate it via four dimensions: Safety, Financial, Operational and Privacy. Using only the likelihood of adverse events it is nearly impossible to quantify cybersecurity risks. Therefore, other criteria related to the attack feasibility are used for evaluating the cybersecurity risks. Such criteria are, for example, attacker skill, needed equipment or window of opportunity. As potential impacts of cyberattacks can be different compared to functional safety, these processes need to be aligned with the organization's risk tolerance.

3.2.1 Functional safety HARA process

Functional safety engineering has been the top priority to eliminate safety risks. ISO 26262 is a sector specific functional safety standard for automotive domain that describes a safety lifecycle for the development of safety-related automotive E/E -systems. Standard provides a well-structured and generic process framework for vehicles E/E -systems safety lifecycle. This includes design, development, production, service process and decommissioning of the product. The purpose of defined processes and methods is to minimize systematic failures during development of E/E -systems and to control random failures during operation. A similar sector specific standard is ISO 25119 that is the functional safety standard for agriculture and forest machinery equipment manufacturers.

The framework in ISO 26262 is structured into several phases. The concept phase starts by defining item(s). The definition is a description of the system containing its functionality, interfaces and environment. After the definition, the HARA (Hazard Analysis and Risk Assessment) analysis is performed for each item. During phase hazardous events and operational situations of the item are identified, categorized and evaluated. ISO 26262 introduced ASIL (Automotive Safety Integrity Level), a new risk classification concept, to help define the necessary safety requirements. ASIL, which is always assigned to an item, is based on the severity, the exposure, and the controllability of the hazardous event. ASIL gets one of the five values ranging from QM (Quality Management) and ASIL A to ASIL D. The D represents the tightest level. A similar concept phase process is introduced in ISO25119. The standard introduced a concept of Agricultural Performance Level (AgPL) for risk evaluation. AgPL gets one of the six values ranging from QM and AgPLa to AgPLe. The AgPLe represents the tightest level.

The result of the concept phase is the functional safety concept and the technical safety concept. The functional safety concept contains top-level safety requirements as safety goals derived from the HARA findings and functional system requirements. The system architecture or the system design requirements are an essential part of the technical safety concept.

3.2.2 Cybersecurity risk management

CPS face security breaches several ways and risk management is challenging due to the complex and evolving threat landscape. Security breaches happen for several reasons. Attacks can happen to people, processes or technology. Risk management systems can be missing, inadequate or failing. Organization needs a comprehensive cybersecurity risk management system to identify unique cybersecurity threats and trends of threats. ISO/SAE 21434 standard for cybersecurity engineering is a fundamental step towards integrating cybersecurity in automotive development processes. The standard provides requirements for framework including cybersecurity processes, E/E -systems security lifecycles (including design, development, production, service process and decommissioning of the product) and a common language for communicating and managing cybersecurity risk. The processes are described from the perspective of a single item. An important aspect of ISO/SAE 21434 is that it defines requirements for framework and process, but it does not define detailed methods how to produce required outcomes.

3.2.3 Cybersecurity and threat modelling process

Threat models can be used to exposure design flaws in security. Threat modeling refers to the process in which specific potential security vulnerabilities and associated risks related to them are identified, so that they can be addressed in a targeted manner. Cyber threats can occur on various levels of the system and affect in many ways to system functions and properties. Threat modeling creates and formalizes a process that can provide information on cybersecurity aspects of system in multiple ways by discovering potential threats, vulnerabilities, and weaknesses.

The concept phase in ISO/SAE 21434 standard is structured into several steps. It starts with item definition. The definition is a description of the system where primary modeling entities are components, functions of the system, data flows and data. These entities become assets when they are combined with security attribute from the CIA - model. Risk treatment has to be evaluated for every security goal using Threat Analysis and Risk Assessment (TARA) which is a systematic approach for threat modeling. TARA activities are performed to identify potential cybersecurity threats to the item, assess the risk associated with the identified threats and determine the paths taken to attack.

ISO/SAE 21434 provides a new classification scheme concept as Cybersecurity Assurance Level (CAL) to support cybersecurity risk value classification. CAL is assigned to an item in the process where discovered threats are mapped to damage scenarios from the road user's perspective and analyze what would be a result from a successful cyber-attack on the item. CAL can get one of four values ranging 1-4 (1 – low to moderate, 2 – moderate, 3 – moderate to high, 4 – high). Concept is similar to ASIL definition in functional safety. Usage of the CAL is not a mandatory requirement of ISO/SAE 21434, and it is introduced in the Annex E of the standard, but classification scheme can be used to specify and communicate a set of assurance requirements. On the other hand, TARA is a requirement of ISO/SAE 21434 standard, and it becomes an integral part of the concept phase. Figure 12 describes the steps of concept phase and TARA process according to ISO/SAE 21434 standard.

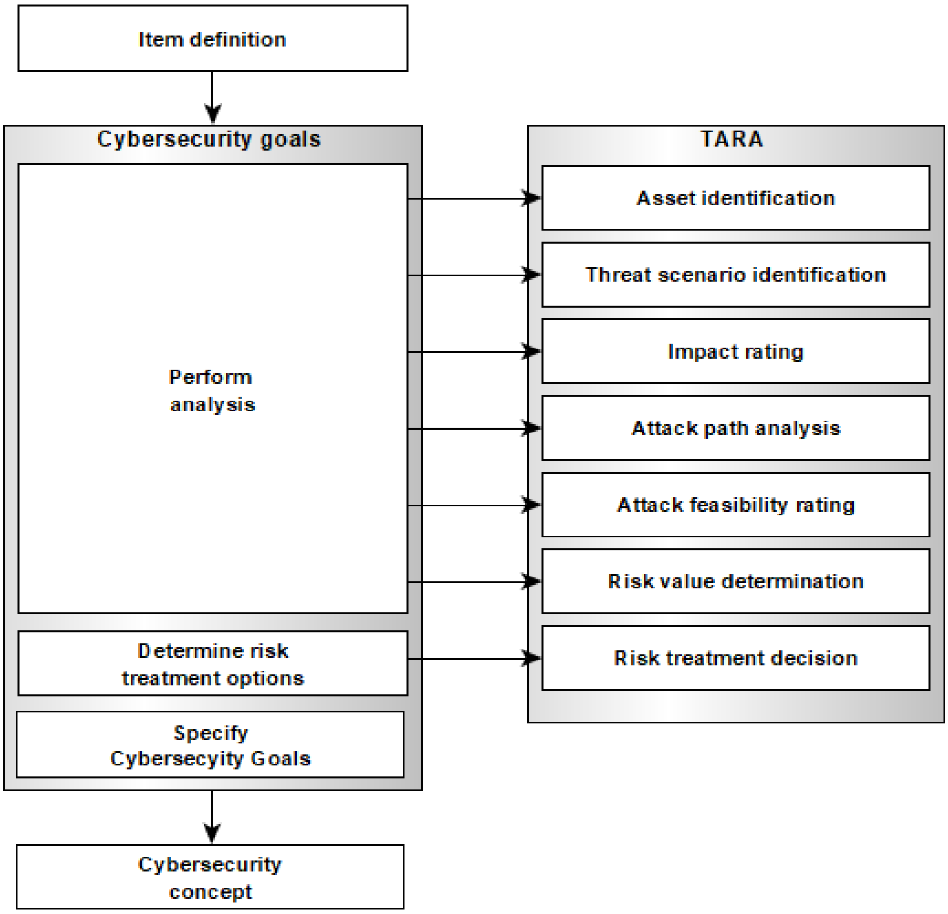

Figure 12. TARA process (based on ISO/SAE 21434)

TARA analysis results with risk treatment decision are captured in cybersecurity goals that is high level cybersecurity objectives definition of item. Cybersecurity goals serve then as the basis for the defining a cybersecurity concept. The cybersecurity concept provides cybersecurity requirements of the item and requirements on the operational environment with associated information on cybersecurity controls.

3.3 Systems engineering lifecycle

During a product development phase V-model is an integral part of vehicles' E/E -architectures development. The V-model is a development model where process is executed in sequential manner in V-shape. The V-model is also called as Verification and validation model, based on the association of a testing phase for each corresponding development stage. The general illustration of the V-model covers activities in the new product development phase that starts from requirements and ends to product validation.

In the end of a product development phase validation ensures that the defined customer requirements are met.

However, this is not enough. The new regulations define requirements for manufacturers to manage the whole product lifecycle from development to decommissioning of the product. Concept and production become integral parts of the product development process. In the automotive engineering functional safety and cybersecurity are independent domains. Both of these domains focus on system-wide features. The product development process benefits if interactions between these domains is defined and necessary co-operation performed during concept development phase.

This research proposes that classical V-model is extended to cover of the product lifecycle also other phases, not only the product development process. In the new vehicle V-model concept phase is also included safety and security engineering activities. In addition, the product concept phase also defines production process requirements in the form of cybersecurity plan. It is a natural extension to validate production process as part of the product development. Figure 13 illustrates this new V-model with combined to engineering process and product lifecycle phases with relevant standards.

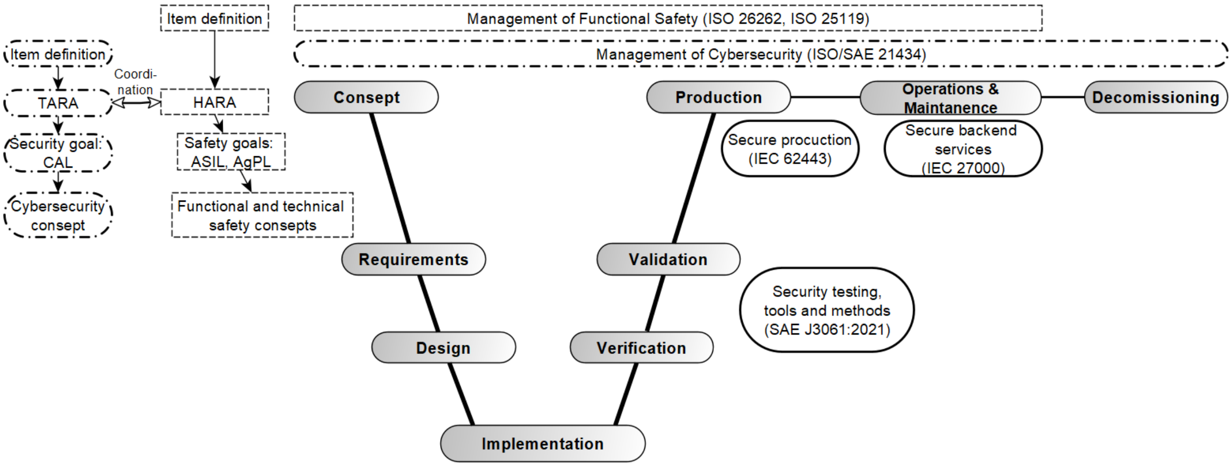

Figure 13. Extended V-model with functional safety and cybersecurity lifecycle

3.4 Vehicle cybersecurity engineering

The ISO/SAE 21434 defines requirements for cybersecurity engineering framework to organizational processes and lifecycle. Secure vehicle systems' realization requires implementation of other standards that provide guidance for engineering secure automotive systems. These automotive systems are in several layers from ITS infrastructure and manufacturers back-end systems to vehicle internal systems. Every layer is a unique domain and has its own assets to protect in connected vehicle cybersecurity architecture. Figure 14 illustrates connected vehicle security layers and assets relation on the layer.

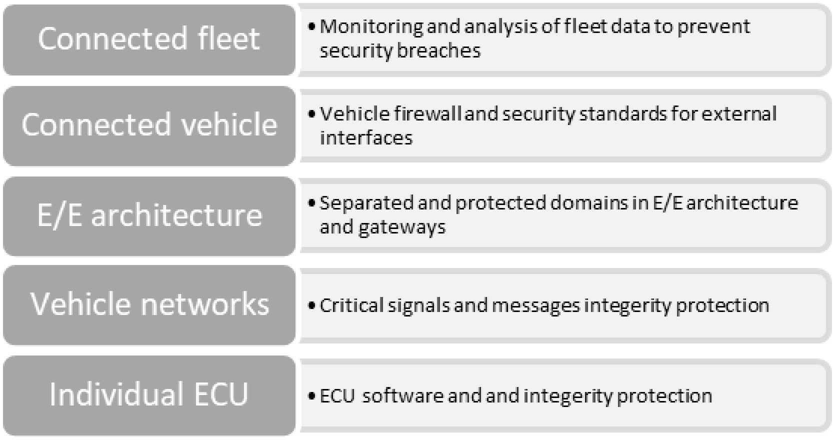
Connected fleet
• Monitoring and analysis of fleet data to prevent security breaches
Connected vehicle
• Vehicle firewall and security standards for external interfaces
E/E architecture
• Separated and protected domains in E/E architecture and gateways
Vehicle networks
• Critical signals and messages integerity protection
Individual ECU
• ECU software and and integerity protection

Figure 14. Connected vehicle security layers and example assets of the layers

There are several standardization organizations developing and providing standards to some areas of the connected vehicle model but there is no comprehensive coordination between all organizations. These standards and their current development status have been introduced in the literature review. The requirements described in the standards are partially overlapping. This makes the vehicle systems development challenging. As an example of overlapping development relates to ITS -systems where ETSI has developed standards as well as ITU-T.

Developed standards lay the foundation for secure vehicle E/E -architecture development. The performed research into standards development can summarized to as an example E/E -architecture for implementation to a real vehicle project with back-end systems. The example E/E -architecture synthesizes the performed research to automotive cybersecurity standards and covers each layer of the connected vehicle architecture that ENISA has described. Figure 15 provides an overview of cybersecurity standards and relation to connected vehicle architecture.

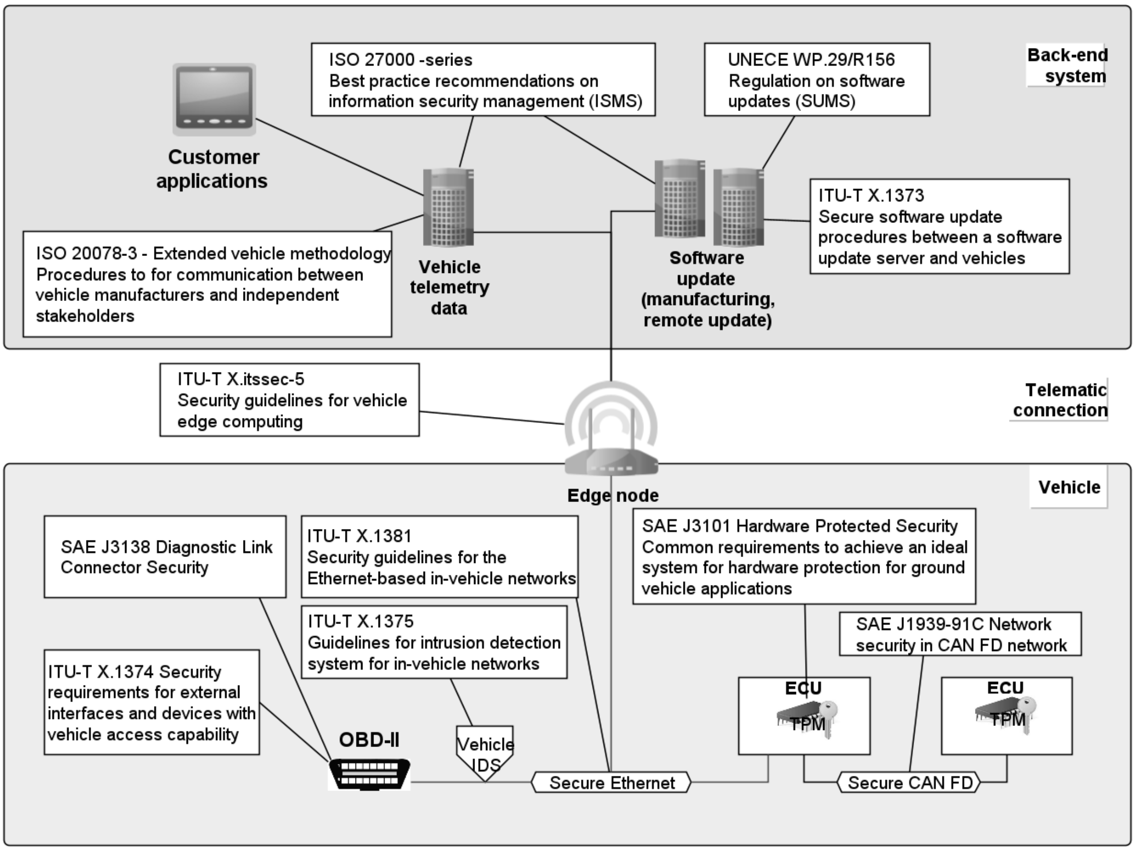
ISO 27000 -series
Best practice recommendations on information security management (ISMS)
UNECE WP.29/R156
Regulation on software updates (SUMS)
Back-end system
Customer applications
ITU-T X.1373
Secure software update procedures between a software update server and vehicles
ISO 20078-3 - Extended vehicle methodology
Procedures to for communication between vehicle manufacturers and independent stakeholders
Vehicle telemetry data
Software update (manufacturing, remote update)
ITU-T X.itssec-5
Security guidelines for vehicle edge computing
Telematic connection
Edge node
Vehicle
SAE J3138 Diagnostic Link Connector Security
ITU-T X.1381
Security guidelines for the Ethernet-based in-vehicle networks
SAE J3101 Hardware Protected Security
Common requirements to achieve an ideal system for hardware protection for ground vehicle applications
ITU-T X.1375
Guidelines for intrusion detection system for in-vehicle networks
SAE J1939-91C Network security in CAN FD network
ITU-T X.1374 Security requirements for external interfaces and devices with vehicle access capability
ECU
TPM
ECU
TPM
OBD-II
Vehicle IDS
Secure Ethernet
Secure CAN FD

Figure 15. Connected vehicle architecture and related standards for product development

4 ORGANIZATIONAL CYBERSECURITY CAPABILITIES EVALUATION TOOL DEVELOPMENT

The objective of this thesis' empirical part is to develop a new artifact as an evaluation tool. The tool is in the form of a questionnaire for interviews to collect stakeholders' knowledge of organizational capabilities of management processes and methods related to cybersecurity perspective. The evaluation tool is designed to follow a structure that derives most of its fundamental components from ISO/SAE 21434 standard framework.

4.1 Organizational cybersecurity capabilities

The proactive approach to cybersecurity management of an organization applies through cybersecurity management system (CSMS). In organizational level CSMS practices relate to the policies and methods that are implemented to management processes. The organization establishes and maintains rules and processes to enable the implementation of the requirements and support the execution of the corresponding activities. On the product level CSMS covers all vehicle lifecycle phases from the concept to development of the product as well as post-development activities such as production, operation, maintenance, and decommissioning.

The main components of CSMS are as follows:

- definition of cybersecurity roles and responsibilities related to product security
- competence management of employees and resources
- cyber risk handling throughout supply chain
- management of product security lifecycle throughout entire lifetime of the product encompassing:
    - early phase and continuous cyber risk assessment
    - secure design and implementation
    - security validation using suitable testing methods
    - continuous security monitoring
    - vulnerability management including incident handling

The aforementioned components may be addressed and documented from different perspectives and objectives. A CSMS might either be integrated as a pillar of a higher-level component, such as a Quality Management System (QMS), or built as an independent set of activities to be interfaced with existing working practices.

A typical CSMS could be segmented into three levels. The first level defines an organization's top level policy. The goal is to formalize on high-level the CSMS scope, its objectives, and specific considerations. This documentation also aims to obtain top management commitment about the importance of product/cyber security.

The second level defines process groups of the organization. The goal is to group and document similar activities. These are based on criteria such as topic, people involved, interfaces with other operations than cyber/product security. These activities need to be described as processes from an operational perspective.

The third level defines supporting resources to ensure the implementation of processes described on higher levels. Supporting resources need to be developed for generating outcomes and records of the process. This level includes different kinds of documentation such as guidelines, forms, templates, tools, etc.

Figure 16 illustrates organizational management levels and CSMS's relation to other management systems dedicated to a specific discipline. A similar approach can applied to building Information Security Management Systems (ISMS) or Software Update Management System (SUMS). SUMS is a systematic approach to define organizational processes and procedures to comply with the requirements for delivery of software updates as set forth in UNECE WP29/R156.

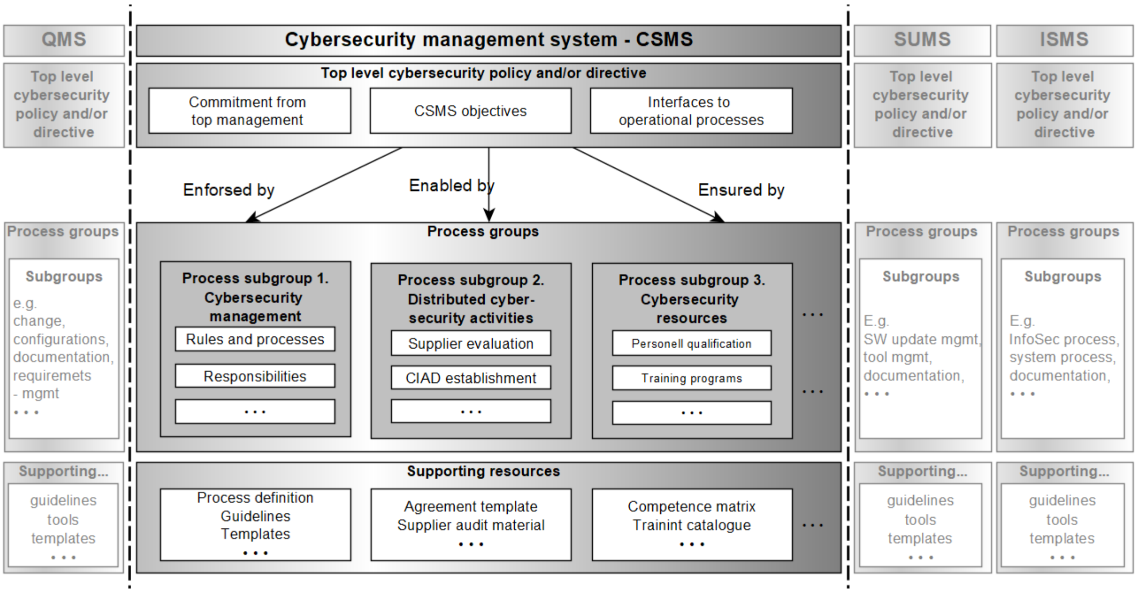
QMS
Top level cybersecurity policy and/or directive
Process groups
Subgroups
e.g. change, configurations, documentation, requiremets - mgmt
• • •
Supporting...
guidelines
tools
templates
• • •
Cybersecurity management system - CSMS
Top level cybersecurity policy and/or directive
Commitment from top management
CSMS objectives
Interfaces to operational processes
Enforsed by
Enabled by
Ensured by
Process groups
Process subgroup 1. Cybersecurity management
Rules and processes
Responsibilities
• • •
Process subgroup 2. Distributed cyber-security activities
Supplier evaluation
CIAD establishment
• • •
Process subgroup 3. Cybersecurity resources
Personell qualification
Training programs
• • •
• • •
• • •
Supporting resources
Process definition
Guidelines
Templates
• • •
Agreement template
Supplier audit material
• • •
Competence matrix
Trainint catalogue
• • •
• • •
SUMS
Top level cybersecurity policy and/or directive
Process groups
Subgroups
E.g. SW update mgmt, tool mgmt, documentation,
• • •
Supporting...
guidelines
tools
templates
• • •
ISMS
Top level cybersecurity policy and/or directive
Process groups
Subgroups
E.g. InfoSec process, system process, documentation,
• • •
Supporting...
guidelines
tools
templates
• • •

Figure 16. Overview of cybersecurity management system (modified from ISO/SAE 21434)

To enable cybersecurity engineering, the organization institutes and maintains cybersecurity governance and a cybersecurity culture. The following questions can be addressed to stakeholders who are involved in organizational cybersecurity management.

- How are the cybersecurity responsibilities arranged at the top management level?
- How is the organizational cybersecurity policy defined in relation to product security?
- What kind of cyber security governance model is used?
- How does an organization establish and maintain rules and processes to enable the implementation of the requirements of used model?
- What activities is implemented to foster and maintain cybersecurity culture?
- How the work products of the product security (for example design documents, test results) are managed?
- Is a organization cybersecurity audit process implemented, and if it is, how?

4.2 Project dependent cybersecurity management

Cybersecurity management of a vehicle project includes planning of the cybersecurity activities used in the vehicle project and allocation of responsibilities. During the project planning phase is created a cybersecurity plan defining which activities will be performed during the project. The cybersecurity plan includes several topics to be considered:

- objective of an activity
- dependencies on other activities or information
- personnel responsible for performing an activity
- required resources for performing an activity
- starting point or end point, and the expected duration of an activity
- identification of the documents to be produced

The cybersecurity case is an input to a cybersecurity assessment and to the release for post development. A cybersecurity case is created to provide an argument for the cybersecurity of the item or component, supported by documents. In distributed development, the cybersecurity case of the item can be a combination of the cybersecurity cases of the customer and cases of the suppliers, which references evidence from the documents generated by both parties.

The cybersecurity assessment judges independently the cybersecurity of an item or component and is an input for the decision to the release for post-development. The cybersecurity assessment includes the cybersecurity plan and all documents identified in the cybersecurity plan, the treatment of the cybersecurity risks and the appropriateness and effectiveness of implemented cybersecurity controls and cybersecurity activities performed for the project.

A cybersecurity assessment report is an independent appraisal of cybersecurity based on the existing evidence and provided rationales. It provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls. The report provides a recommendation for acceptance, conditional acceptance, or rejection of the cybersecurity of the item or component. The report also provides the acceptance conditions for a conditional acceptance. Figure 17 describes the relationships between the organizational level cybersecurity management and project level cybersecurity activities.

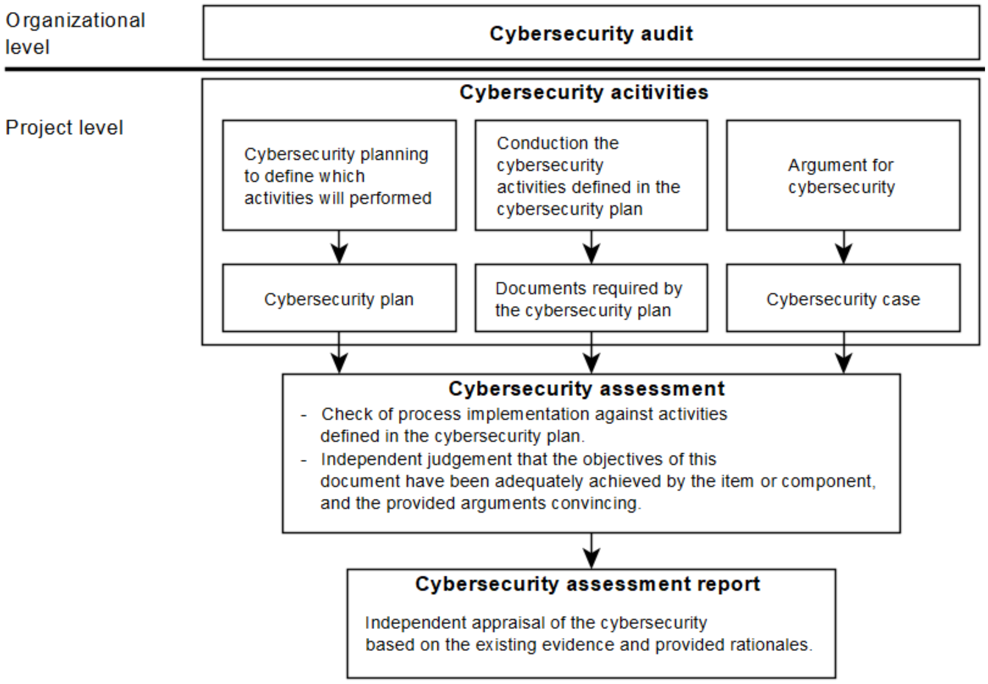
Organizational level
Cybersecurity audit
Project level
Cybersecurity acitivities
Cybersecurity planning to define which activities will performed
Conduction the cybersecurity activities defined in the cybersecurity plan
Argument for cybersecurity
Cybersecurity plan
Documents required by the cybersecurity plan
Cybersecurity case
Cybersecurity assessment
- Check of process implementation against activities defined in the cybersecurity plan.
- Independent judgement that the objectives of this document have been adequately achieved by the item or component, and the provided arguments convincing.
Cybersecurity assessment report
Independent appraisal of the cybersecurity based on the existing evidence and provided rationales.

Figure 17. Project organizational cybersecurity activities (modified from ISO/SAE 21434)

The following questions can be addressed to stakeholders related to project cybersecurity responsibilities and planning.

- How are cybersecurity activities responsibilities of the project are assigned?
- Is a cybersecurity plan created during project planning and is the plan communicated?
- What is the content of the project cybersecurity plan?
- How are the cybersecurity plans regarding their respective cybersecurity activities and interfaces defined for a situation in which cybersecurity activities are partly distributed further to a client or a supplier?

The questions below can be addressed to stakeholders related to cybersecurity case and assessment.

- How does project planning define project relevant cybersecurity cases?
- What cybersecurity assessment activities are included in the project planning phase?
- Are resources reserved to plan and perform a cybersecurity assessment?

A project dependent cybersecurity activity may be tailored. If a tailored cybersecurity activity is used, then a rationale needs to be provided and reviewed why the tailoring is adequate and sufficient to achieve the relevant objectives. Part of the tailoring activities can be performed by another entity in the supply chain. These activities are not considered as tailored, but they are part of distributed cybersecurity activities.

Reuse of items and components is a possible development strategy. It can be applied with or without modifications to an item, component, or their operational environment. However, modifications can introduce vulnerabilities that might not have been considered for the original item or component. A reuse analysis of an item or component includes several activities. The manufacturer must first identify the modifications to the item or component and the modifications of its operational environment. Second, analyze the cybersecurity implications of the modifications, including the effects on the validity of cybersecurity claims and previously made assumptions. Third, identify the affected or missing documents. Fourth, specify the cybersecurity activities necessary to conform the cybersecurity plan. The following questions related to tailoring cybersecurity activities and reuse of components can be addressed to stakeholders.

- Are tailored cybersecurity activities used and documented?
- Are tailored cybersecurity activities objectives defined?
- Have tailored cybersecurity activities the rationale why the tailoring is adequate and sufficient to achieve the relevant objectives?
- Is a reuse analysis of an item or component performed and documented?
- If exists, how reuse analysis evaluates whether this is sufficient to support the integration of an item or component?

A post-development report decides whether the item or component can be, from a cybersecurity perspective, released for post-development. The following questions can be addressed to stakeholders related to post-development.

- What project planning activities are included for post-development?
- How post-development requirements of the item or component are defined and accepted?

4.3 Distributed cybersecurity activities

Distributed cybersecurity activities with component suppliers deal with cyber risk handling throughout a full supply chain. This has an impact on every supplier that provides security critical items or components. Cybersecurity relevant requirements need to be defined and provided to supply chain to ensure end-to-end security across the supply chain.

The automotive product manufacturer is responsible for that its component suppliers' cybersecurity activities are aligned with those of the manufacturer. This can be done by collecting enough evidence of qualifying suppliers and approving suppliers by proving their capabilities to develop, operate and maintain the security of supplied components throughout whole vehicle lifecycle. The alignment of responsibilities for distributed cybersecurity activities between customers and suppliers can be secured through interface agreements. The following questions can be addressed to for stakeholders related to distributed cybersecurity activities.

- How are supplier candidate’ cybersecurity engineering capabilities evaluated to develop and perform post development activities of security critical items?
- What cybersecurity goals, relevant to the item or component in question, are included in a request for quotation?
- Is a cybersecurity interface agreement made with all customers and suppliers prior to starting the distributed cybersecurity activities for security critical items?
- What distributed cybersecurity activities are defined in a cybersecurity interface agreement?

4.4 Continual cybersecurity activities

Continual cybersecurity activities are performed during all the phases of the product lifecycle and can be done outside of a specific project. Cybersecurity monitoring collects cybersecurity information and analyses the cybersecurity information for triage based on defined triggers. The information can be collected from internal sources such as cybersecurity claims, cybersecurity specifications, threat scenarios, past vulnerability analyses, information received from the field. Examples of external sources are researchers, the organization’s supply chain and customers of the organization.

A cybersecurity event evaluation determines if the cybersecurity event presents a weakness for an item or component. Each vulnerability corresponding cybersecurity risks needs to be managed. Vulnerability management tracks and oversees the treatment of identified vulnerabilities in items and components until their end of cybersecurity support. Questions related to continual cybersecurity activities can be addressed to stakeholders.

- What cybersecurity information is collected and triaged?
- How are cybersecurity events evaluated to identify weaknesses in an item and/or component?
- What weakness analyzing methods are used, if any?
- How a vulnerability management process is implemented, if any?

4.5 Concept phase activities

The concept phase means consideration of vehicle level functionalities when there is limited amount of system specific knowledge available. The aim of system concepting is to gain knowledge about the system and the risks related to this system. The process of concepting starts defining high-level functional models of the system. These models are used to define high-level cybersecurity aspects of the system.

4.5.1 Item definition

Automotive systems are implemented using items. The system and its purpose can be illustrated using high-level block diagram and used technology stacks. These represent items capsulated to its boundaries from an operational environment and functional perspective in the context of cybersecurity. The function of the item describes intended behavior of the item during the lifecycle phases. The item definition forms the basis for the subsequent activities. The following questions can be addressed to stakeholders related to item definition.

- How is an item defined in relation to its boundary definition, functions and preliminary architecture?
- Is the information about the operational environment of the item described, and if yes, how?

4.5.2 Cybersecurity goals

Cybersecurity goals are the highest level of requirements that are derived from and formulated for each of the highest risk threats. The goals are documented in the TARA. A cybersecurity goal is a requirement to protect assets against a threat scenario. Risk treatment options shall be determined for each threat scenario in accordance with risk treatment decision. The following questions can be defined for stakeholders related to setting cybersecurity goals.

- How is a risk analysis of the item performed?
- What cybersecurity goals of an item are determined based on threat scenario risk treatment options?
- How is verification of cybersecurity goals performed?

4.5.3 Cybersecurity concept

The cybersecurity concept consists of cybersecurity requirements and requirements on the operational environment. Both are derived from the cybersecurity goals and based on a comprehensive view of the item. Technical and/or operational cybersecurity controls and their interactions to achieve the cybersecurity goals need to be described considering dependencies between the functions of the item. The description can include conditions for achieving cybersecurity goals and functions dedicated to addressing specific aspects of threat scenarios. The description can also serve to evaluate designs and to determine cybersecurity validation targets. The following questions can be addressed to stakeholders related to concept definition.

- How are cybersecurity requirements of the item and requirements on the operational environment defined based on cybersecurity goals?
- How is a verification of the cybersecurity concept performed?

4.6 Product development phase

The secure development of automotive items relates to managerial activities and documentations provided by the organization. These cybersecurity activities are performed iteratively until no further refinements of cybersecurity controls are needed. The cybersecurity specifications are defined and confirmed through verification activities for the fulfilment of the cybersecurity concept.

4.6.1 Design

Cybersecurity specifications are defined based on specifications from higher levels of architectural abstraction, cybersecurity controls that is selected for implementation and existing architectural design. Cybersecurity specifications include the specification of interfaces between sub-components of the defined architectural design related to the fulfilment of the defined cybersecurity requirements. The cybersecurity specifications can include the identification of configuration and calibration parameters relevant for fulfilling the cybersecurity requirements. Cybersecurity specification may also consider cybersecurity implications of post-development phases. The following questions can be addressed to stakeholders related to cybersecurity design.

- Is the cybersecurity specification included in the product development process?
- What is the content of the cybersecurity specification?
- How the architectural design is analyzed to identify weaknesses in architecture?
- Are the cybersecurity requirements defined and allocated to components of the architectural design?

- What procedures are specified to ensure cybersecurity after the development of the component?
- What verification methods are defined into cybersecurity specification?

4.6.2 Integration and verification

Integration and verification activities verify that the implementation and integration of components fulfill the defined cybersecurity specifications. The activities specification for integration and verification considers several elements:

- the defined cybersecurity specifications
- the configurations intended for series production
- sufficient capability to support the functionality defined in the cybersecurity specifications
- the conformity with the modelling, design, and coding guidelines

Methods for verification can include following elements: requirements-based test, interface test, resource usage evaluation, verification of the control flow and data flow, dynamic analysis and static analysis.

If verification by testing is adopted, test coverage shall be evaluated using defined test coverage metrics to determine sufficiency of the test activities. Standard test coverage metrics can be inadequate for cybersecurity, for example, statement coverage for software. Software testing confirms that unidentified weaknesses and vulnerabilities remaining in the component are minimized. Testing methods can include the following activities: functional testing, vulnerability scanning, fuzz testing, penetration testing.

In cybersecurity validation activities the item is considered in its operational environment at the vehicle level with the series production configurations. The objectives of validation are in two main categories: achievement of the cybersecurity goals and validity of the cybersecurity claims and confirm that the item achieves the cybersecurity goals and unreasonable risks do not remain. The validation activities include several tasks. Review of all managed risks, reviewing the work products to confirm cybersecurity goals achievement, demonstrate adequacy and achievement of cybersecurity goals by performing penetration testing. The following questions can be addressed to stakeholders related to item cybersecurity verification and validation.

- What kind of integration and verification activities are implemented in order the component to fulfil the defined cybersecurity specifications?
- What are the defined coverage metrics to determine sufficiency of the test activities?
- What kind of validation activities in vehicle the level have been implemented?

4.7 Post development phases

The security engineering activities expand the product process beyond the concept and development phases to the post development phases, including also the decommissioning phase of the product. New UNECE WP.29 regulations force automotive manufacturers to patch security weaknesses and continuous system cybersecurity (incident) monitoring process in the operations and maintenance phase of the product lifecycle.

4.7.1 Production

Production covers the manufacturing and assembly of an item or component, including the vehicle level. A production control plan is created to ensure that cybersecurity requirements for post development are applied to the item or component and to ensure that vulnerabilities cannot be introduced during production.

The production control plan includes the following:

- The sequence of the steps that are applied to the cybersecurity requirements for post-development
- The production tools and equipment
- The cybersecurity controls to prevent unauthorized alteration during production

- Methods to confirm that the cybersecurity requirements for post-development are met

The following questions can be addressed to stakeholders related to production.

- What is cybersecurity content of the production control plan?
- Is the production control plan implemented to the organization?

4.7.2 Operations and maintenance

Updates are changes made to an item or component during post development. Updates can include additional information, for example technical specifications, integration manuals and user manuals. Organizations can issue updates for various reasons, for example, addressing vulnerabilities or safety issues, providing functional improvements.

A cybersecurity incident response occurs when an organization invokes it as part of vulnerability management. A cybersecurity incident response plan for each cybersecurity incident needs to be created. The plan includes remedial actions of the incident with assigned responsibilities, method for determining progress, incident response closure criteria and communication plan for internal and external stakeholders. The following questions can be addressed to stakeholders related to operations and maintenance.

- What kind of cybersecurity incident response plan has been defined?
- Is the incident response plan implemented to organization?
- What kind of process is implemented to field updates?
- How update-related capabilities (tools, skills) are maintained?

4.8 End of cybersecurity support and decommissioning

Decommissioning is different from the end of cybersecurity support. An organization can end cybersecurity support for an item or component, but that item or component can still function in the field as designed. End of cybersecurity support and decommissioning are considered in the concept and product development phases.

It is needed to communicate with customers when an organization decides to end cybersecurity support for an item or component. Communication procedure needs to be created to handle decommissioning communication. The following questions can be addressed to stakeholder related to decommissioning.

- What are the procedures to communicate the end of cybersecurity support of product?
- What are the cybersecurity relevant procedures to decommissioning of product?

5 DISCUSSION

Modern vehicles have changed from electromechanical systems to cyber physical systems. This ongoing trend towards automation and connectivity makes connected vehicles attractive targets for cyber-attacks and protections against cyber-attacks have become even more important. The research aim of the study was to investigate cybersecurity management processes of connected vehicles.

5.1 Status of automotive industry regulations and standards

The first research question for the study was: What is the status of automotive industry regulations and standards related to cybersecurity? In March 2021 the United Nations Economic Commission for Europe (UNECE) WP.29 (World Forum for Harmonization of Vehicle Regulations) committee published two new regulations of road vehicles' type approval: R155 for cybersecurity and R156 for software update. Based on this, the European Commission has set new rules in the new Vehicle General Safety Regulation (GSR) to improve road safety (European Parliament Council of the European Union, 2019). It is mandatory for car manufacturers and suppliers in UNECE countries to meet GSR regulations for all new vehicle types to homologate new vehicle types as of 6th June 2022 and it will become mandatory for all vehicles produced as of July 2024 (Costantino et al., 2022). GSR set new requirements for management systems and cybersecurity measures that vehicle manufacturers have to implement. Car manufacturers have forced to proactive approach for cybersecurity via organization management practices (European Union Agency for Cybersecurity, 2019). The methods of these practices relate to organizations' capability to vehicles' lifecycle management over the whole vehicle lifetime. UNECE WP.29/R155 regulation does not determine car manufacturers how to secure their vehicles. Instead, it outlines management actions that have to be taken. The regulation consists of the requirement to implement Cyber Security Management System (CSMS) to organization management practices (UNECE, 2021a).

SAE International and ISO have developed ISO/SAE 21434 standard for automotive cybersecurity engineering. Purpose of standard is to provide guidelines for CSMS implementation to organization management practices including cybersecurity risk management (ISO/SAE 21434, 2021). Standard provides requirements for management and engineering processes of the E/E -systems from the vehicles cybersecurity perspective, including the participants in the supply chain. Standard requirements provide the basis for the company-specific processes and practices development.

Automotive systems are in several layers of the connected vehicle model, ranging from Intelligent Transport System (ITS) infrastructure and manufacturers' back-end systems to vehicles' internal systems (European Union Agency for Cybersecurity, 2019). Every layer is a unique domain and has its own assets to be protected in a connected vehicle cybersecurity architecture. Several standardization organizations have recently provided standards related to cybersecurity in automotive domain to improve vehicles' cybersecurity. The realization of secure vehicle system requires implementation of standards that provide guidance for engineering secure automotive systems.

SAE has published and is still working with several standards in different areas of automotive cybersecurity. These areas cover vehicles' internal networks and hardware protections, diagnostic connector security as well as security testing methods. As an example SAE J3101 defines implementation requirements for hardware protected security for ground vehicles and SAE J3138 for diagnostic connector security (SAE J3138, 2018; SAE J3101, 2020). ITU-T has provided several security recommendations for the Intelligent Transport System (ITS) concept. ITU-T Recommendations X.1372-1375 focus on vehicle-to-everything (V2X) communication, vehicles' internal systems, and security of these systems. ISO has developed the Extended Vehicle (ExVe) concept for accessing vehicle data and its interfaces (ISO 20077, 2017; ISO 20078:2021, 2021). The extended vehicle concept consists of a physical road vehicle with external software and hardware extensions that are developed, implemented and managed by the vehicle manufacturer. IEC 62443 and ISO 27000 - standards series are not originally developed for automotive systems engineering, but they are becoming ever more critical for production cloud-connected service infrastructure (Dobaj et al., 2021). These international standard series are relevant for automotive industry to be used organization IT -infrastructure, back-end systems and production operational technology (OT) that covers network technology which control production process and equipment (IEC 62443 series n.d.; ISO 27002, 2018).

These regulations and standards provide guidelines for cybersecurity framework implementation to management framework, connected vehicle architecture and their back-end systems.

5.2 Connected vehicles cybersecurity risk management

The second research question for the study written: How to manage cybersecurity risk of connected vehicles? According to the study material risk management is not one time event. Instead, it is a continuous organization process to response uncertainty that can impact on operations' outcomes. The risk management process itself contains several steps. Risk identification is the process of identifying and assessing threats to an organization including its operations and workforce. Risk analysis involves evaluating the probability that a risk event might occur and the potential outcome of each event. A risk assessment is a process to identify potential hazards and analyze what can happen if a hazard occurs (Aven, 2016). Risk treatment is the process of selecting and implementing measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk (Hopkin, 2018). Cybersecurity deals with risk management via risk quantification. The typical approach for impact rating is to evaluate it on four dimensions: Safety, Financial, Operational and Privacy. Using only the likelihood of adverse events it is nearly impossible to quantify cybersecurity risks. Therefore, other criteria related to the attack feasibility are used for evaluating the cybersecurity risks for example attacker skill, needed equipment or window of opportunity. According to Zayane (2022) automotive cyber-secure engineering answers to question that how everything can be secured to such an extent that risks can be managed as well as possible. In the automotive domain CSMS covers organizations' policies and processes for handling cyber risks related to the entire lifecycle of vehicles. ISO/SAE 21434 standard provides requirements for framework (ISO/SAE 21434, 2021). This includes requirements for cybersecurity processes, E/E -systems security lifecycles including design, development, production, service process and decommissioning of the product and a common language for communicating and managing cybersecurity risk. However, ISO/SAE 21434 standard does not define detailed methods how to produce required outcomes.

According to the sources used in this study cyber threats can occur on various levels of the system and can affect many ways to system functions and properties. Threat modeling refers to the process in which specific potential security vulnerabilities and associated risks related to them are identified, so that they can be addressed in a targeted manner. Threat Analysis and Risk Assessment (TARA) is a systematic approach for threat modeling. TARA activities are performed to identify potential cybersecurity threats to the item, assess the risk associated with the identified threats and determine the paths taken to attack. TARA analysis results with risk treatment decision are captured in cybersecurity goals that is high level cybersecurity objectives definition of item. The cybersecurity goals serve then as the basis for defining the cybersecurity concept. The cybersecurity concept provides cybersecurity requirements of the item and requirements on the operational environment with associated information on cybersecurity controls (ISO/SAE 21434, 2021). TARA is a requirement of ISO/SAE 21434 standard, and it becomes an integral part of the cybersecurity risk management activities in the product process concept phase.

5.3 Organization product security management

The third research question for the study was written: How connected vehicles affect organization management related to product cybersecurity? United Nations regulation UNECE WP.29/R155 and ISO/SAE 21434 standard and are essential steps towards integrating cybersecurity in automotive management practices. ISO/SAE 21434 on cybersecurity defines a set of requirements that needs to be fulfilled by vehicle manufacturers, suppliers and service providers, covering the entire vehicle lifecycle from the vehicle development to its decommissioning (ISO/SAE 21434, 2021). Via GSR the European Commission set new requirements for management systems. UNECE WP.29/R155 requires that OEMs have to implement cybersecurity process framework called Cyber Security Management System (CSMS) (UNECE, 2021a). The responsible vehicle manufacturer in the process is named Original Equipment Manufacturer (OEM). ISO/SAE 21434 standard’s purpose is to provide guidelines for CSMS implementation to organization management practices including cybersecurity risk management. ISO/SAE 21434 standard itself provides only a generic framework and it addresses the cybersecurity perspective in engineering.

According to research sources, typical CSMS could be segmented into three levels. The first level defines an organization’s top level policy. The goal is to formalize on high-level the CSMS scope, its objectives, and specific considerations. This documentation also aims to obtain top management commitment about the importance of product/cyber security. The second level defines process groups of the organization. The goal is to group and document similar activities, based on criteria like topic, people involved, interfaces with other activities than cyber/product security. These activities need to be described as processes from an operational perspective. The third level defines supporting resources to ensure the implementation of processes described on higher levels. Supporting resources need to be developed for generating outcomes and records of the process.

Since June 2022, the implementation of the CSMS has become a prerequisite for car manufacturers to claim for a new type approval. To get new vehicle type approval vehicle manufactures have to follow a three steps approach in accordance with UNECE UNECE WP.29/R155. First, vehicle manufacturers must demonstrate to authorities their implementation of CSMS. It is mandatory to have the CSMS audited by authorities and get a CSMS certificate to prove that a vehicle manufacturer has organizational capability to fulfill the requirements (UNECE, 2021a).

Second, when CSMS is certified by an authority, a vehicle manufacturer has a right to apply for Vehicle Type Approvals (VTA) (UNECE, 2021a). During this phase authorities require the manufacturer to demonstrate the implementation of processes described within the CSMS for this specific vehicle type program or specific vehicle. It is necessary to provide documentation demonstrating the implementation of vehicle security processes implementation, for example for risk assessment process.

The third step is to maintain authorization. Even though the VTA for a vehicle has been authorized, the manufacturer must maintain the authorization in order to continue selling the vehicle on the market. Manufacturers have to regularly (once a year) provide provision report for authorities (UNECE, 2021a). The main objective of this reporting is to demonstrate for the authorities that protection measures are still effective and adequate against evolving threat landscape. This report is the outcome of the manufacturer’s cybersecurity monitoring activities, information related to new cyber-attacks and potential incidents that may require adjustment of cybersecurity measures.

This study developed an evaluation tool in the form of a questionnaire that can be used to collect information from organizations on what is the currents status of the capabilities for comprehensive cybersecurity management process. The tool is based on ISO/SAE 21434 standard, and by performing interviews the stakeholders may analyze which organizational activities of the cybersecurity management system framework are already on the level of requirements. Questions for organizational evaluation is provided in appendix 1 of the thesis.

6 CONCLUSIONS

Modern vehicles are the implementation of CPS, and they are connected to information network all the time. That makes them tempting targets for cyberattacks. Connected vehicles' cybersecurity is a fast-developing domain and organizations have to implement new proactive working practices to mitigate risks that are rising daily from cybersecurity events and incidents. This thesis study was aimed to investigate cybersecurity and management processes of connected vehicles. The focus has been on the field of cybersecurity in automotive domain.

Car manufacturing is a leader in automotive domain, and the practices used in the car manufacturing influence also to other type of road vehicle manufacturers. In 2021 United Nations Economic Commission for Europe (UNECE) WP.29 (World Forum for Harmonization of Vehicle Regulations) committee published two new regulations of road vehicles type approval. Regulations set new requirements for automotive industry management systems. Car manufacturers in UNECE countries have to implement cybersecurity process framework called Cyber Security Management System (CSMS) to organizational management practices. It covers organizations policies and processes for handling cyber risks related to the entire lifecycle of vehicle. The European Commission has set new requirements in the new vehicle General Safety Regulation (GSR) to improve road safety. GSR forces a proactive approach for cybersecurity via organizational management practices. The methods of these practices relate to organizations capability to vehicles lifecycle management over the whole vehicle lifetime. The GSR rules will first apply to new vehicle types, and they have to fulfill for claiming for new type approvals as of June 2022.

ISO/SAE 21434 standard provides the state of art requirements for cybersecurity management framework and engineering process to meet current UNECE regulations in automotive industry. Connected vehicles cybersecurity deals with cyber risk management methods and processes to reduce vehicle risk to other road users. In the automotive domain CSMS covers organizations' policies and processes for handling cyber risks related to the entire lifecycle of vehicles. The ISO/SAE 21434 engineering standard is a cornerstone for product security management practices. The standard provides requirements for CSMS framework. This includes requirements for cybersecurity processes, E/E -systems security lifecycles including design, development, production, service process and decommissioning of the product and a common language for communicating and managing cybersecurity risk. The elements of ISO/SAE 21434 standard do not prescribe an execution of the individual topics because the implementation can be based on a method that is defined in other standards or domain specific guidelines. Instead, it is defining a framework for the company-specific process and practice specification. Implementation of the CSMS is audited by authorities, and it is part of the vehicle type homologation process. The standard defines threat modelling as method for cybersecurity risk management. Threat Analysis and Risk Assessment (TARA) is a systematic approach for threat modeling and TARA activities becomes an integral part of the product process concept phase cybersecurity risk management activities.

To enable cybersecurity engineering, the organization institutes and maintains cybersecurity governance and a cybersecurity culture. This involves specifying organizational policy, rules and processes that enable the implementation of cybersecurity activities. The responsibilities of the cybersecurity activities and corresponding authorities need to be assigned to perform activities. Many standardization organizations have recently provided cybersecurity standards related to connected vehicles. These standards provide guidelines for cybersecurity implementation to automotive products E/E -architecture.

The empirical part of this thesis developed a new artifact, an evaluation tool in the form of questionnaire. The stakeholders can use the tool to collect information and analyze a specific organization's current status of the organizational capabilities for comprehensive cybersecurity management process.

6.1 Limitations

The development of the questionnaire raised limitations. The elements of ISO/SAE 21434 standard set requirements to cybersecurity management system but do not prescribe practical implementation of such system. Practical implementation of CSMS can be based on a method that is defined in other standards or domain specific guidelines. This needs to be considered when the results of the questionnaire are analyzed and generalized outside of car manufacturing, for example in agricultural equipment manufacturing who provide vehicles for offroad and public roads.

6.2 Further research

The organizational processes in cybersecurity is a broad topic and opens new research possibilities. Recommendations for further research.

The CSMS also has elements of the organization strategic effectiveness. Implementation variants of the CSMS to current management system like Quality Management Systems (QMS) are intrinsically not critical for reaching compliance, but they might have a strong impact on organization effectiveness. Further research on strategic efficiency measurement would be needed for CSMS governance viewpoint.

The developed questionnaire provides an evaluation tool to collect management practices on all organization levels and in different functions. Data can be collected from strategy to product portfolio management including decommissioning of the product in the end of product lifecycle. The empirical data collection can be performed by selecting stakeholders or security champions from different organizational levels, functions, and business units. This type of study could be performed as a case study research.

REFERENCES

Andress, J., 2014. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Second Edition. Syngress Publishing.

Antille, D. L., Chamen, T., Tullberg, J. N., Isbister, B., Jensen, T. A., Chen, G., Baillie, C. P. and Schueller, J. K., 2018. Controlled traffic farming in precision agriculture. *In*: *Precision agriculture for sustainability*. Cambridge, United Kingdom: Burleigh Dodds Science Publishing, 239–270.

Aven, T., 2016. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253 (1), 1–13.

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A. and Aggoune, E. H. M., 2019. Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk. *IEEE Access*, 7, 129551–129583.

Benke, K. and Tomkins, B., 2017. Future food-production systems: Vertical farming and controlled-environment agriculture. *Sustainability: Science, Practice, and Policy*, 13 (1), 13–26.

Bokan, B. and Santos, J., 2021. Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures. *In*: *2021 Systems and Information Engineering Design Symposium (SIEDS)*. IEEE, 1–6.

British Standards Institution, 2022. *Standards and regulation* [online]. Available from: https://www.bsigroup.com/en-GB/standards/Information-about-standards/standards-and-regulation/ [Accessed 12 Feb 2023].

Bronwen, M. and Karen, Y., 2007. *An Introduction to Law and Regulation : Text and Materials.* Cambridge, UK: Cambridge University Press.

Collin, J. and Saarelainen, A., 2016. *Teollinen internet*. Helsinki: Tallentum.

Costantino, G., Vincenzi, M. De and Matteucci, I., 2022. A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434. *In*: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 340–347.

Dobaj, J., Macher, G., Ekert, D., Riel, A. and Messnarz, R., 2021. Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*.

European Parliament Council of the European Union, 2019. REGULATION (EU) 2019/2144 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. *Official Journal of the European Union*, PE/82/2019/REV/1, L 325/1-L 325/40.

European Union Agency for Cybersecurity, 2019. *ENISA good practices for the security of smart cars*. European Union Agency for Cybersecurity.

Gowda, D. V., Prabhu, S. M., Ramesha, M., Kudari, J. M. and Samal, A., 2021. Smart Agriculture and Smart Farming using IoT Technology. *Journal of Physics: Conference Series*, 2089 (1).

Hopkin, P., 2018. *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Fifth edition. London, UK: Kogan Page Limited.

Hornbogen, F., 2020. *Standards and norms for automotive cybersecurity* [online]. Itemis. Available from: https://www.security-analyst.org/relevant-standards-and-norms-for-automotive-cybersecurity/ [Accessed 21 Apr 2022].

IEC 61508, 2010. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems Part 1-7*. International Electrotechnical Commission IEC.

IEC 62443 series, n.d. *Industrial communication networks and system security*. International Electrotechnical Commission IEC.

Inglis, C., 2016. Cyberspace-Making Some Sense of It All. *Source: Journal of Information Warfare*, 15 (2), 17–26.

ISO 20077, 2017. *Road Vehicles - Extended vehicle (ExVe) methodology*. International Organization for Standardization ISO.

ISO 20078:2021, 2021. *Road vehicles - Extended vehicle (ExVe) web services*. International Organization for Standardization ISO.

ISO 23132:2020, 2020. *Road vehicles — Extended Vehicle (ExVe) time critical applications — General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS)*. International Organization for Standardization ISO.

ISO 25119, 2018. *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*. International Organization for Standardization ISO.

ISO 26262, 2018. *Road vehicles - Functional safety Part 1-10*. International Organization for Standardization ISO.

ISO 27000 series, 2018. *Information technology - security techniques*. International Organization for Standardization ISO.

ISO 27002, 2018. *Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization ISO.

ISO/IEC 15408, 2009. *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security*. International Organization for Standardization ISO.

ISO/SAE 21434, 2021. *Road vehicles - Cybersecurity engineering*. ISO/SAE International.

ISO/TR 23791:2019, 2019. *Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series*. International Organization for Standardization ISO.

ITU X.1372, 2020. *Security guidelines for vehicle-to-everything (V2X) communication*. International Telecommunication Union -Telecommunication standardization sector ITU-T.

ITU X.1373, 2017. *Secure software update capability for intelligent transportation system communication devices*. International Telecommunication Union - Telecommunication standardization sector ITU-T.

ITU X.1374, 2020. *Security requirements for external interfaces and devices with vehicle access capability*. International Telecommunication Union - Telecommunication standardization sector ITU-T.

ITU X.1375, 2020. *Guidelines for an intrusion detection system for in-vehicle networks*. International Telecommunication Union -Telecommunication standardization sector ITU-T.

ITU X.1381, 2021. *Security guidelines for the Ethernet-based in-vehicle networks*. International Telecommunication Union -Telecommunication standardization sector ITU-T, SG17.

ITU X.itssec-5, 2021. *Security guidelines for vehicular edge computing*. International Telecommunication Union -Telecommunication standardization sector ITU-T, SG17.

ITU-T, 2022. *Intelligent transport system (ITS) security* [online]. Available from: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q13.aspx [Accessed 5 Dec 2022].

Kure, H. I., Islam, S. and Razzaque, M. A., 2018. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, 8 (6).

Lehto, M., 2015. Phenomena in the Cyber World. *In*: *Cyber Security: Analytics, Technology and Automation*. Cham, Switzerland: Springer, 3–29.

Lehto, M., 2018. Cyberspace and Cyber Warfare. *In*: *Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures*. Amsterdam, Netherlands: IOS Press, 99–109.

Mahmood, A., Siddiqui, S. A., Sheng, Q. Z., Zhang, W. E., Suzuki, H. and Ni, W., 2022. Trust on wheels: Towards secure and resource efficient IoV networks. *Computing*, 104 (6), 1337–1358.

Marty, K., 2021. *UNECE WP.29 / R155 – How Cyber Security will impact the automotive market as of June 2022* [online]. Available from: https://certx.com/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/ [Accessed 25 Oct 2022].

Merriam-Webster, 2022. *'Cyberspace'* [online]. Dictionary, Merriam-Webster. Available from: https://www.merriam-webster.com/dictionary/cyberspace [Accessed 18 Mar 2022].

Möller, D. and Haas, R., 2019. *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications*. Cham, Switzerland: Springer.

Rondelli, V., Franceschetti, B. and Mengoli, D., 2022. A Review of Current and Historical Research Contributions to the Development of Ground Autonomous Vehicles for Agriculture. *Sustainability*, 14 (15), 9221.

SAE J3061_202112, 2021. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Society of Automotive Engineers SAE.

SAE J3101, 2020. *Hardware Protected Security for Ground Vehicles*. Society of Automotive Engineers SAE.

SAE J3138, 2018. *Diagnostic Link Connector Security*. Society of Automotive Engineers SAE.

SAE J3254, 2023. *Automotive Cybersecurity Maturity Model Best Practice*.

Saiz-Rubio, V. and Rovira-Más, F., 2020. From smart farming towards agriculture 5.0: A review on crop data management. *Agronomy*, 10 (2), 207.

Schallmo, D., Williams, C. A. and Lang, K., 2018. An Integrated Design Thinking Approach – Literature Review, Basic Principles and Roadmap for Design Thinking. *In*: *ISPIM Innovation Symposium*. Manchester, UK: The International Society for Professional Innovation Management (ISPIM), 1–18.

Schmittner, C. and Macher, G., 2019. Automotive Cybersecurity Standards - Relation and Overview. *In*: *Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings 38*. Springer International Publishing, 153–165.

Solomon, M. and Chapple, M., 2005. *Information security illuminated*. Sudbury, MA: Jones and Bartlett Publichers, Inc.

Tekniikka & Talous, 2021. Benjamin Särkkä auttaa hakkerina yrityksiä – ”Järjestelmään hyökätään joka tapauksessa”. *Tekniikka & Talous* [online], 2021. Available from: https://www.tekniikkatalous.fi/uutiset/benjamin-sarkka-auttaa-hakkerina-yrityksia-jarjestelmaan-hyokataan-joka-tapauksessa/dd03f83c-8c8e-4dde-86a7-ba744e535870 [Accessed 18 Jan 2022].

Thomasson, J. A., Baillie, C. P., Antille, D. L., Lobsey, C. R., McCarthy, C. L. and others, 2019. Autonomous technologies in agricultural equipment: a review of the state of the art. *In*: *ASABE Distinguished Lecture Series, No. 40*. St. Joseph, MI, USA: American Society of Agricultural and Biological Engineers, 1–17.

UNECE, 2021a. *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. Geneva. No. Regulation Addendum 154 – UN Regulation No. 155.

UNECE, 2021b. *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. Geneva. No. Regulation Addendum 155 – UN Regulation No. 156.

UNECE, 2022. *WP.29 - Introduction | UNECE* [online]. Available from: https://unece.org/wp29-introduction [Accessed 25 Sep 2022].

United Nations, D. of E. and S. A. P. D., 2019. *World Population Prospects 2019*. No. Volume II: Demographic Profiles (ST/ESA/SER.A/427).

University of Massachusetts Amherst, 2022. *Standards* [online]. Available from: https://guides.library.umass.edu/c.php?g=719645&p=5126968 [Accessed 16 Feb 2023].

Venable, J. and Baskerville, R., 2012. Eating our own cooking: Toward a more rigorous design science of research methods. *Electronic Journal of Business Research Methods*, 10 (2), 141–153.

Whitman, M. and Mattord, H., 2019. *Management of Information Security*. Sixth Edition. Boston, USA: Cengage Learning, Inc.

Zayane, A., 2022. *CySec, FuSa, TARA, HARA, ASIL Functional safety vs. cybersecurity in the automotive industry* [online]. Available from: https://www.cyres-consulting.com/functional-safety-vs-cybersecurity-in-the-automotive-industry/ [Accessed 24 Jan 2023].

APPENDIX 1 Questions for organizational evaluation

Theme 1: Cybersecurity organizational management

1. How are the cybersecurity responsibilities arranged at the top management level?
2. How is the organizational cybersecurity policy defined in relation to product security?
3. What kind of cyber security governance model is used?
4. How does an organization establish and maintain rules and processes to enable the implementation of the requirements of used model?
5. What activities is implemented to foster and maintain cybersecurity culture?
6. How the work products of the product security (for example design documents, test results) are managed?
7. Is a organization cybersecurity audit process implemented, and if it is, how?

Theme 2: Project dependent cybersecurity management

1. How are cybersecurity activities responsibilities of the project are assigned?
2. Is a cybersecurity plan created during project planning and is the plan communicated?
3. What is the content of the project cybersecurity plan?
4. How are the cybersecurity plans regarding their respective cybersecurity activities and interfaces defined for a situation in which cybersecurity activities are partly distributed further to a client or a supplier?
5. How does project planning define project relevant cybersecurity cases?
6. What cybersecurity assessment activities are included in the project planning phase?
7. Are resources reserved to plan and perform a cybersecurity assessment?
8. Are tailored cybersecurity activities used and documented?
9. Are tailored cybersecurity activities objectives defined?
10. Have tailored cybersecurity activities the rationale why the tailoring is adequate and sufficient to achieve the relevant objectives?
11. Is a reuse analysis of an item or component performed and documented?

12. If exists, how reuse analysis evaluates whether this is sufficient to support the integration of an item or component?
13. What project planning activities are included for post-development?
14. How post-development requirements of the item or component are defined and accepted?

Theme 3: Distributed cybersecurity activities

1. How are supplier candidate' cybersecurity engineering capabilities evaluated to develop and perform post development activities of security critical items?
2. What cybersecurity goals, relevant to the item or component in question, are included in a request for quotation?
3. Is a cybersecurity interface agreement made with all customers and suppliers prior to starting the distributed cybersecurity activities for security critical items?
4. What distributed cybersecurity activities are defined in a cybersecurity interface agreement?

Theme 4: Continual cybersecurity activities

1. What cybersecurity information is collected and triaged?
2. How are cybersecurity events evaluated to identify weaknesses in an item and/or component?
3. What weakness analyzing methods are used, if any?
4. How a vulnerability management process is implemented, if any?

Theme 5: Concept

1. How is an item defined in relation to its boundary definition, functions and preliminary architecture?
2. Is the information about the operational environment of the item described, and if yes, how?
3. How is a risk analysis of the item performed?
4. What cybersecurity goals of an item are determined based on threat scenario risk treatment options?

5. How is verification of cybersecurity goals performed?
6. How is risk analysis of the item performed?
7. What cybersecurity goals of an item are determined based on threat scenario risk treatment options?
8. How is verification of cybersecurity goals performed?
9. How are cybersecurity requirements of the item and requirements on the operational environment defined based on cybersecurity goals?
10. How is a verification of the cybersecurity concept performed?

Theme 6: Product development phase

1. Is the cybersecurity specification included in the product development process?
2. What is the content of the cybersecurity specification?
3. How the architectural design is analyzed to identify weaknesses in architecture?
4. Are the cybersecurity requirements defined and allocated to components of the architectural design?
5. What procedures are specified to ensure cybersecurity after the development of the component?
6. What verification methods are defined into cybersecurity specification?
7. What kind of integration and verification activities are implemented in order the component to fulfil the defined cybersecurity specifications?
8. What are the defined coverage metrics to determine sufficiency of the test activities?
9. What kind of validation activities in vehicle the level have been implemented?

Theme 7: Post development phases

1. What is cybersecurity content of the production control plan?
2. Is the production control plan implemented to the organization?
3. What kind of cybersecurity incident response plan has been defined?
4. Is the incident response plan implemented to organization?
5. What kind of process is implemented to field updates?
6. How update-related capabilities (tools, skills) are maintained?

7. What are the procedures to communicate the end of cybersecurity support of product?
8. What are the cybersecurity relevant procedures to decommissioning of product?